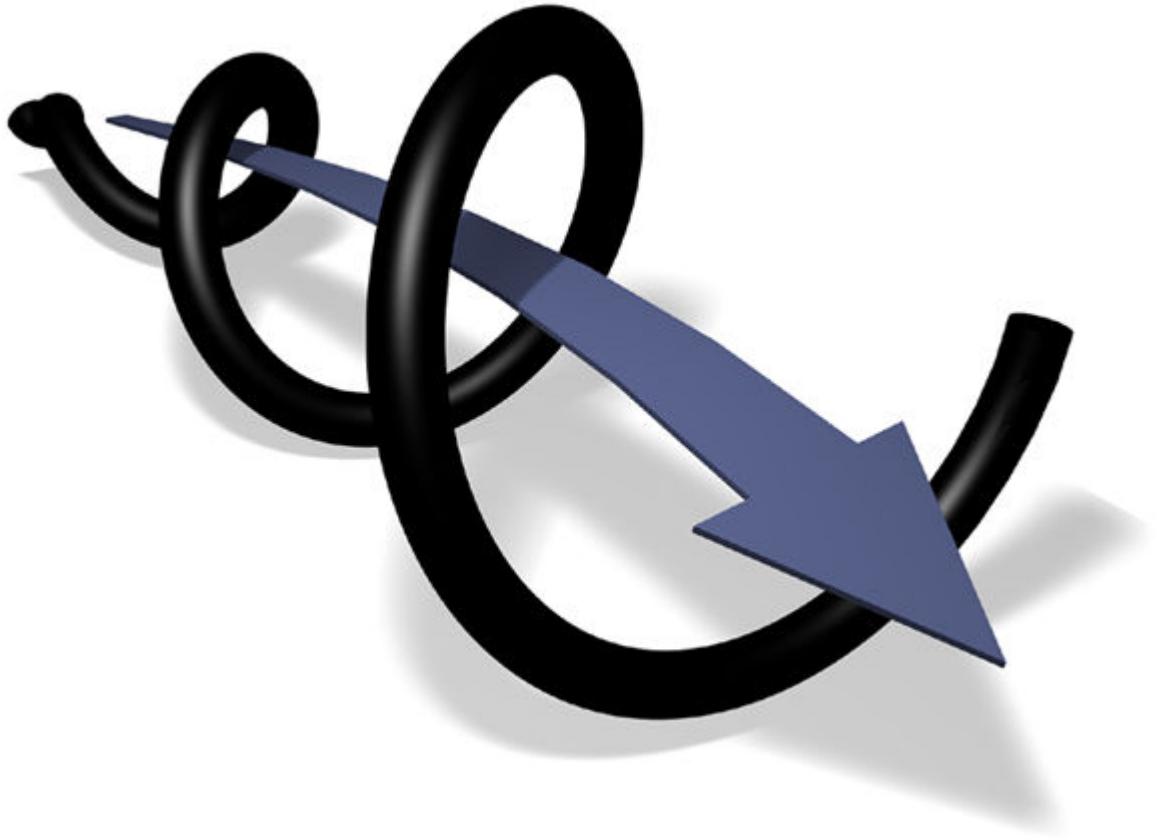
# InJoy Firewall™ 4.0

## Getting Started



# Contents


**1. INTRODUCTION ..... 4**
1.1. Document Scope ..... 4
1.2. Reading This Document ..... 4

**I. Setting up the software 5**

**2. INSTALLATION ..... 6**
2.1. System Requirements ..... 6
2.2. Before installation ..... 6
2.3. Graphical Installation ..... 8
2.4. Scripted installation ..... 12
2.5. Uninstalling InJoy Firewall™ ..... 13
**3. STARTING AND STOPPING THE FIREWALL ..... 15**
3.1. Understanding the Desktop Folder ..... 15
3.2. Starting the InJoy Firewall™ Server ..... 18
3.3. Starting the InJoy Firewall™ GUI ..... 21
3.4. Starting the InJoy Firewall™ Deskbar Application ..... 22
3.5. Stopping the InJoy Firewall™ ..... 23
**4. BASIC CONFIGURATION ..... 25**
4.1. Inserting the License Key ..... 26
4.2. Verifying Internal Network Configuration ..... 27
4.3. Selecting Plugin Features ..... 28
4.4. Other Firewall Properties ..... 29
4.5. Finishing the Configuration ..... 31

**II. Graphical Administration 32**

**5. THE USER INTERFACE ..... 33**
5.1. Introducing the Firewall GUI ..... 33
5.2. Managing the GUI Look and Feel ..... 36
5.3. Basic GUI Commands ..... 39
5.4. Basic Statistics and Information Monitors ..... 40
5.5. Advanced Firewall GUI Monitors ..... 45
5.6. Remote Firewall Administration ..... 48
**6. THE FIREWALL DESKBAR ..... 52**
6.1. Introducing the Firewall Deskbar ..... 52
6.2. Firewall Deskbar Configuration ..... 53
6.3. Using the Firewall Deskbar ..... 55
6.4. Firewall Deskbar FAQ ..... 58

**III. Working with the InJoy Firewall™ 59**

**7. MORE ABOUT CONFIGURATION ..... 60**
7.1. Plugin Architecture ..... 60
7.2. InJoy Firewall™ Configuration ..... 61
7.3. Plain-text Configuration ..... 63
7.4. Activating Configuration Changes ..... 63
**8. USING THE INJOY FIREWALL™ ..... 65**
8.1. Verifying Basic Firewall Operation ..... 65
8.2. Checking Firewall Logs ..... 67
8.3. Managing Firewall Security ..... 68
8.4. Firewall Performance Tuning ..... 79
8.5. Using Dynamic IP Addresses ..... 81
8.6. Firewall Packet Tracing ..... 82

8.7. Creating a Firewall Watchdog ..... 84

# IV. Networking with the InJoy Firewall™ 85

**9. SETTING UP AN INTERNET GATEWAY ..... 86**
9.1. Using Network Address Translation (NAT) ..... 86
9.2. Deploying a Small Network ..... 89
9.3. Network Deployment Example ..... 90
9.4. Creating Demilitarized Zones (DMZs) ..... 95

# V. References 97

**10. APPENDIX A - UTILITY PROGRAMS ..... 98**
10.1. Sync ..... 98
10.2. Ipformat ..... 99
10.3. IPGate ..... 100
10.4. Logview ..... 101
**11. APPENDIX B - SUMMARY OF CONFIGURATION FILES ..... 103**
11.1. General Properties ..... 103
11.2. Firewall Plugin Configuration ..... 103
11.3. DHCP Server Configuration ..... 104
11.4. IPSec Configuration ..... 104
11.5. PPPoE Configuration ..... 105
11.6. PPTP Configuration ..... 105
**12. APPENDIX C - CONFIGURATION ATTRIBUTES ..... 106**
12.1. Firewall Properties ..... 106
**13. APPENDIX D - COMMAND LINE PARAMETERS ..... 111**
13.1. InJoy Firewall™ Server ..... 111
13.2. InJoy Firewall™ GUI ..... 111
**14. APPENDIX E – USING MULTIPLE NICS ..... 113**
14.1. Installing Multiple Firewalls ..... 113
14.2. Starting Multiple Firewall Servers ..... 114
14.3. Managing Multiple Firewall Servers ..... 114

# 1 Introduction

With the InJoy Firewall™ you can finally say good-bye to the old-generation Firewall solutions that were difficult to manage and welcome to the intuitive, intelligent and complete solution that focus on today's busy professionals.

The InJoy Firewall™ is designed to be user-friendly and offer the flexibility and features that beginners, power-users, consultants, businesses and large enterprises need.

## 1.1. Document Scope

This "Getting Started" document provides a concise description of the InJoy Firewall™ installation, configuration and basic operation.

Advanced plugin features, such as the InJoy Firewall™ Security customization and IPSec VPNs are introduced, however, for in-depth coverage of these plugins, please refer to the feature specific configuration guides.

Topics are covered with minimal Operating System dependence. Screen-shots are mostly from Windows XP, but may appear from any OS platform.

## 1.2. Reading This Document

To ease your navigation, this document has been divided into several distinct parts according to the amount of information different types of readers are likely to need:

**Part I.** Setting up the Software
**Part II.** Graphical Administration
**Part III.** Working with the Firewall
**Part IV.** Networking with the Firewall
**Part V.** References

Part I by itself contains enough information to successfully install and use the InJoy Firewall™. Users who want a better understanding of the Firewall can consult the remaining Parts for additional information.

# Part I
# Setting up the software

# 2 Installation

Installation of the InJoy Firewall™ is an extremely straightforward process, designed to be easy-to-perform for beginners, while providing flexibility for expert and business users.

## 2.1. System Requirements

The minimum system requirements for the InJoy Firewall™ are:

| | |
|---|---|
| **Processor:** | Pentium class PC or 100% compatible |
| **Operating System:** | Windows 2000/2003/XP/Vista, Linux kernel 2.4 or 2.6, OS/2 3.0 or later, eComStation 1.0 or later |
| **Memory:** | 32 megabytes memory |
| **Disk Space:** | 100 megabytes free disk space |
| **Network Adapter:** | At least one 10/100Mbit Ethernet adapter |

Please consult the platform-specific README file for additional installation requirements and details related to installation on a particular operating system.

## 2.2. Before installation

To install the InJoy Firewall™, follow these steps:

| Step 1: | Step 2: | Step 3: | Step 4: |
|---|---|---|---|
| Download the InJoy Firewall™ from F/X Communications. | Uninstall un-used or conflicting networking products. | Close all running programs. | Start the installation. |

### Starting the installation

To start the installation, you must first choose among two possible methods.

- **Graphical Installation.**
  Graphical installation is available in Windows and OS/2. Through a series of dialogs, you will be guided through the installation process.

  To execute the graphical installation, you must download the InJoy Firewall™ as an executable (".exe") file.
- **Scripted Installation.**
  The InJoy Firewall™ includes command files for every supported platform, allowing scripted installation and un-installation.

**Note:** Under Linux, scripted installation is the only available installation method. Under Windows and OS/2, scripted installation is an optional alternative to using the graphical InJoy Firewall™ Installer described in section 2.3.

## What is the Windows Logo Testing Alert?

When installing the InJoy Firewall™ for the first time, Microsoft Windows may display one or more messages indicating that the installed components have not undergone Windows Logo testing. Do not be alarmed if you see a few (or even a lot) of these messages.


The exact number of warning messages depends on the number of existing network bindings and network cards installed into the system. Typically 1 to 3 of these messages needs to be acknowledged, but on advanced systems, as many as 16 warnings have been seen.

The Windows Logo testing alert is a standard message to inform that the device drivers being installed have not been tested by Microsoft. To accept, click **Yes** or **Continue**, depending on the version of Windows being used.

For automatic or silent deployment, Windows offers you to turn off the driver signing check in the menu: "**Control Panel | System Properties | Hardware | Driver Signing**" – as shown below.


On Windows Vista, different message is displayed to the user, which only asks acceptance of F/X Communications signed device driver. It may also be displayed several times, unless you tick the "Don't ask anymore for F/X Communications signed drivers". There's currently no way to ensure unattended way of installing the drivers on Windows Vista.

With this information, you are ready to start the installation.

## 2.3. Graphical Installation

The InJoy Firewall™ Installer will guide you through a series of dialogs asking for details about the way in which the InJoy Firewall™ should be installed.

| Step 1: | Step 2: | Step 3: | Step 4: |
|---|---|---|---|
| Choose installation directory. | Choose network adapter to firewall. | Enable IP Forwarding. | Finish the installation. |

## Step 1: Choose installation directory


Select a directory in which to install the InJoy Firewall™. Use the file system browser to navigate to a folder using your mouse, or manually enter the directory where the InJoy Firewall™ should be installed. Click **Next** when you are ready to have the InJoy Firewall™ files copied to your hard drive.

- **Updating an existing Installation**
  If you are updating an existing Installation of the InJoy Firewall™, the installer will prompt you to overwrite existing InJoy Firewall™ files. If you choose **Yes** or **All**, the new version of InJoy Firewall™ will be installed over the old one, keeping your existing configuration files. Security settings and license information will remain intact, with one exception (see next paragraph).

  The InJoy Firewall™ system rules are overwritten by the installer when a new version of the InJoy Firewall™ is installed. If you wish to preserve changes you have made to the pre-defined Security Levels, you should either make your changes in a custom Security Level or preserve the files in the firewall\rulelib subdirectory. Refer to the "Firewall Security Guide" for more information about Security Levels.

- **Clean Installation**
  For novice users, clean installation of the InJoy Firewall™ to an empty directory is recommended. New versions of the InJoy Firewall™ may offer new default values or new configuration settings which were not available in previously installed versions.

## Step 2: Choose network adapter to firewall

Several configuration tasks must be performed at this dialog:


**Select a network adapter.**
In the drop-down box, select the network adapter that is connected to the insecure network—typically your Internet Service Provider (ISP).

If your system contains multiple externally connected network cards, you will need to install multiple instances of the InJoy Firewall™ — one per insecure network interface. For more information about multiple Firewall installations, please refer to Section 14.1, "Installing Multiple Firewalls."

Along with the listed network cards, you will also see "Dial-Up" appearing as an adapter that can be firewalled. Select "Dial-Up" if you need the Firewall to protect Windows dial-up networking connections. The Firewall will automatically bind to any active dial-up connection, regardless of which connection profile you are dialing.

Note: If network adapters show up incorrectly in the drop-down box, the installer's auto-detection has failed. Possible causes include conflict with other software or operating system malfunction. To resolve the problem, it is recommended that you consult the platform specific readme file and ultimately contact F/X's support department.

**Configure passive security.**
The InJoy Firewall™ installs a low-level device driver to intercept IP traffic (at the lowest level) and transport it to the Firewall application for processing. When the Firewall Server is stopped, the device driver offers two possible modes of operation:

- **Allow all IP traffic.** The device driver will transparently allow traffic through the firewall when the Firewall Server application is not running. Choose this to be able to stop the Firewall Server without losing the ability to use the insecure network interface. This is the default choice.
- **Block all IP traffic.** The device driver will NOT allow traffic through the firewall when the Firewall Server application is not running. This setting is recommended for high-security systems through which insecure traffic must never pass – even if this means a halt to all traffic until the Firewall Server can be restarted.

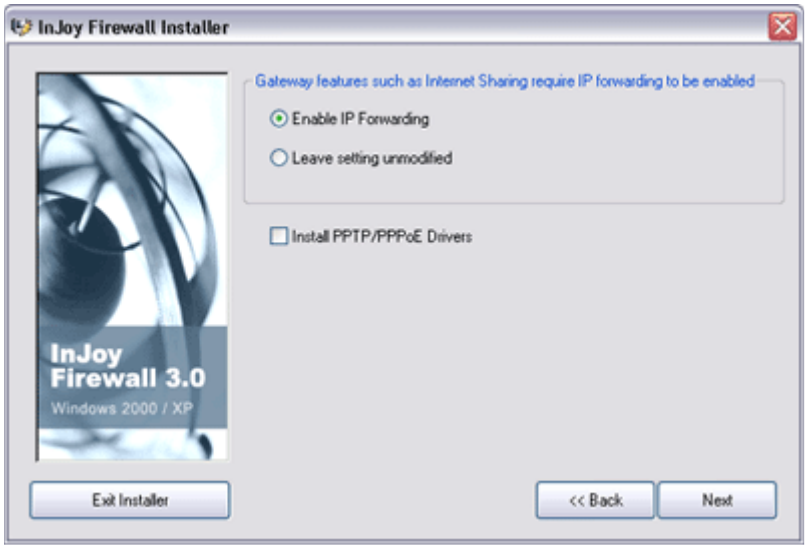
**Choose a firewall launch method.**
The InJoy Firewall™ Server can be started in one of two ways:

- **Automatically at system boot.** Choose this option to start the Firewall Server at system boot or as a Windows Service – on the Windows operating systems.
- **Manually.** Choose this option to start the Firewall Server application manually from the desktop folder, or by using the command prompt, each time you want the firewall to run.

**Note:** You can safely run the installation multiple times in succession to easily change the above options - even without uninstalling.

Click **Next** when you are ready to proceed to the next dialog.

## Step 3: IP Forwarding and PPPoE/PPTP Support




**IP Forwarding**
When IP forwarding is enabled, it allows IP packets to be routed between network interfaces, effectively turning your Firewall PC into a powerful network router. The InJoy Firewall™ requires IP Forwarding to be enabled in order to serve as an Internet gateway for an internal network.

The IP forwarding setting may be changed at any time using the "IPGate" tool.

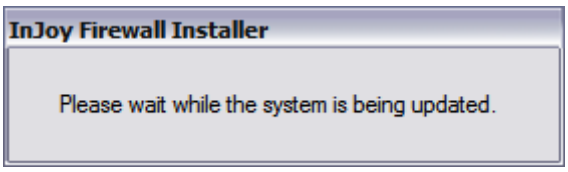
**Install PPPoE/PPTP Drivers**
Enable the "Install PPPoE/PPTP Drivers" checkbox in the above dialog if you plan on using the Firewall for PPPoE or PPTP connections.

Installing the PPPoE and PPTP drivers will not harm your system. However, during installation the additional drivers may cause you to see more "Unsigned Driver" Warnings from the Windows operating system.

Click **Next** when you are ready to proceed to the next dialog.

### Step 4: Finishing the Installation

After leaving the IP Forwarding dialog, the installer will proceed to install the InJoy Firewall™ device drivers and update your desktop. A notice is displayed to indicate that the system is being updated.




When the system is finished being updated, the below dialog will appear:


**Installation Complete**
Congratulations! The InJoy Firewall™ has now been installed!

You should now reboot the system to activate any updated device drivers or changes to the IP Forwarding configuration.

## 2.4. Scripted installation

### Installation Scripts

There are several scripts related to installation and removal of the InJoy Firewall™ product. They are:

| Name of Script | Description |
|---|---|
| install.bat (Windows)<br>install.cmd (OS/2)<br>Install.sh (Linux/FreeBSD) | Installs the Firewall device drivers, prompts for a network interface and creates the desktop folder. |
| uninstal.bat (Windows)<br>uninstal.cmd (OS/2)<br>Uninstall.sh (Linux/FreeBSD) | Removes the InJoy Firewall™ from the Operating System. Files and directories should be manually deleted. |
| folder.bat (Windows) | Creates the desktop folder. You may run |

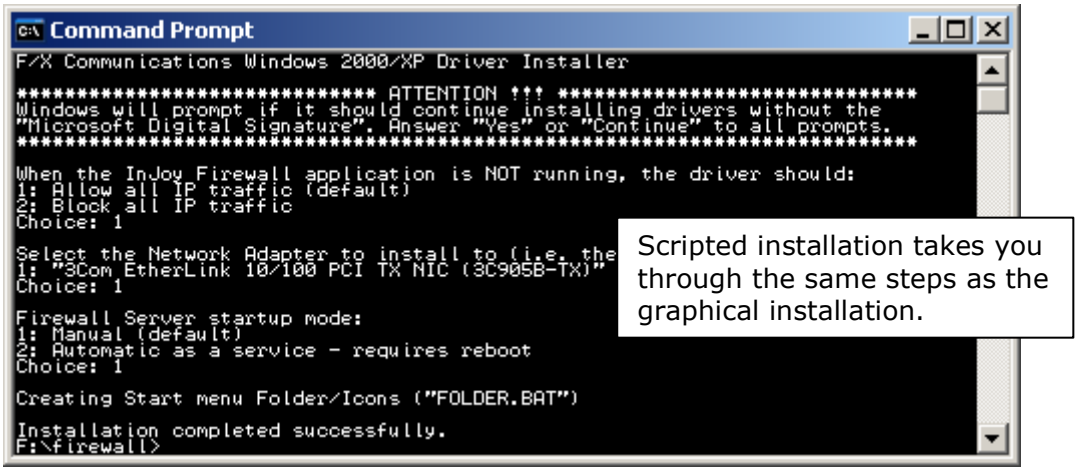
| | |
|---|---|
| folder.cmd (OS/2)<br>Folder.sh (Linux/FreeBSD) | this script at any time and in succession. |

### Why use scripted installation?

There are a several benefits to choosing scripted installation rather than GUI-based installation. Scripted installation allows you to:

- Externally control the installation, by making the install script part of other scripts or processes
- Install InJoy Firewall™ remotely, using only a simple telnet or ssh session
- Quickly install and uninstall the InJoy Firewall™ on machines without an installed graphical user interface

Below you can see the scripted installation in action:




Scripted InJoy Firewall™ installation, performed at a command prompt, is also quick and simple.

## 2.5. Uninstalling InJoy Firewall™

There are two ways to remove an installation of the InJoy Firewall™:

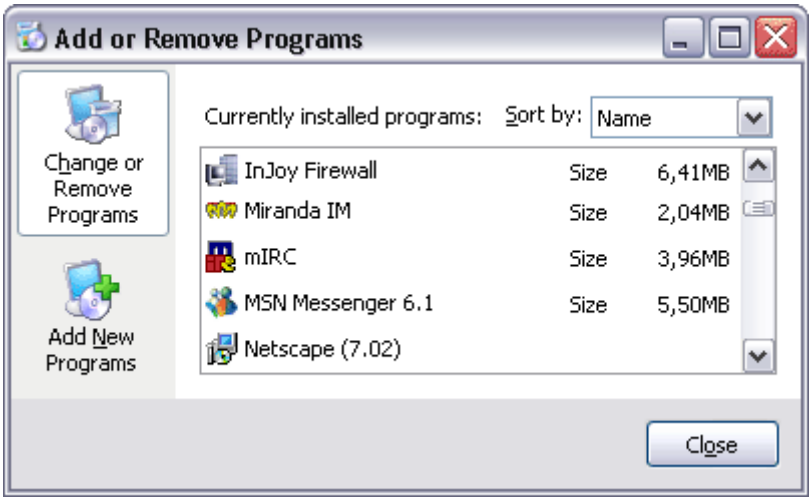
- Using the uninstall script
- using the graphical uninstaller

For details on removing the InJoy Firewall™ using the uninstall script, please refer to Section 2.4, "Scripted installation."

### Graphical Uninstallation

To launch the graphical uninstaller in Windows or OS/2, select the **Uninstall** item in the **Extras** sub-folder of the InJoy Firewall™ desktop folder. The graphical uninstaller will appear. To begin the removal process, click on the **Begin** button.

On Windows, it is also possible to use the "**Control Panel | Add or Remove Programs**" to start uninstallation:




In the removal process, all InJoy Firewall™ files are deleted and the InJoy Firewall™ device drivers are removed from the operating system. Log files and other files that weren't part of the original InJoy Firewall™ distribution remain intact.

# 3 Starting and Stopping the Firewall

Once you have installed the InJoy Firewall™ and the desktop folder has been created, you can start to use the Firewall Server and related tools.

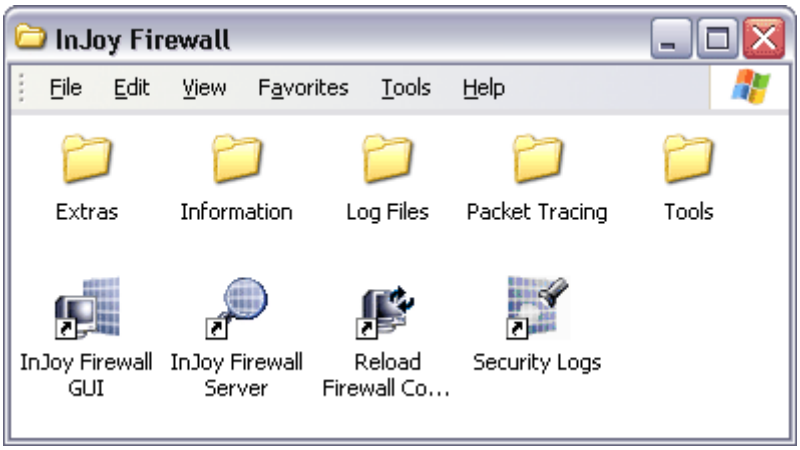
| Step 1: | Step 2: | Step 3: | Step 4: |
|---|---|---|---|
| Understanding the InJoy Firewall™ Desktop Folders. | Starting the InJoy Firewall™ Server. **(IMPORTANT)** | Starting the InJoy Firewall™ GUI. (OPTIONAL) | Starting the Firewall Toolbar application. (OPTIONAL) |

## 3.1. Understanding the Desktop Folder

When the InJoy Firewall™ is installed, a comprehensive program folder is created in the **start menu** of Windows.

In other Operating Systems, the folder is created directly on the desktop. Throughout this manual, the term "desktop folder" is used to describe both folder types.

### The Main Desktop Folder



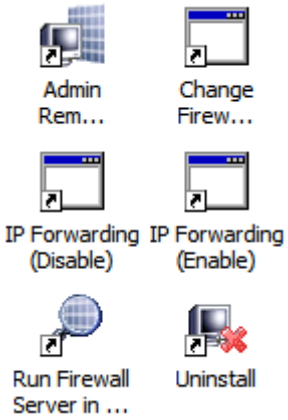

From the desktop folder, you can easily start the Firewall and perform numerous common networking tasks.

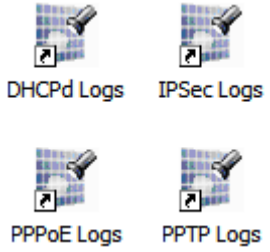
The icons which appear in the desktop folder are:

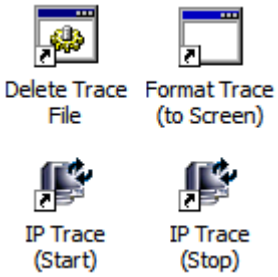
| Products | | Icon Description |
|---|---|---|
|  InJoy Firewall Server | gateway.exe | The **InJoy Firewall Server** icon launches the Firewall Server application. When this application is running, your network is protected.<br><br>On one flank, the Firewall Server uses low-level device driver technology to intercept network traffic – and on the other edge, it loads modular feature plugins to perform specialized tasks on the captured network traffic. |
|  InJoy Firewall GUI | fgui.exe | The **InJoy Firewall GUI** icon launches the optional Firewall GUI application.<br><br>Using this application, you can manage all the major features of the Firewall Server from the local desktop or remotely over TCP/IP.<br><br>The Firewall GUI enjoys a one-to-one relationship with the Firewall Server. To manage multiple Firewall Servers, multiple GUIs must be started. |
|  Security Logs | logview.exe | The **Security Logs** icon launches the customizable Log Viewer, providing a single location for integrated Firewall log file viewing. The Log Viewer can monitor pre-configured sets of log files or custom log files based on custom Firewall rules. |
|  Reload Firewall Co... | sync –firewall | The **Reload Firewall Configuration** icon causes the Firewall Server to activate changes to the InJoy Firewall™ security settings. These changes can be made through the Firewall GUI or directly in the firewall* plain text configuration files. |

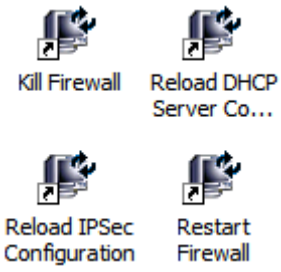
Note that on UNIX based platforms, the commands must be entered without the trailing ".EXE" extension.

## Desktop Sub-folders

| Sub-folder → Extras | Icon Description |
|---|---|
|  | The **Admin Remote Firewall** icon starts the InJoy Firewall™ GUI and prompts for the IP address and password of a remote InJoy Firewall™. |
| | The **Change Firewall Adapter** icon allows you to select the network adapter on which the Firewall Server operates. |
| | **The IP Forwarding Disable/Enable** icon sets the status of the IP Forwarding option. IP Forwarding is a separate system setting that controls whether network traffic is routed between network interfaces. |
| | The **Run Firewall Server in Background** icon executes the Firewall Server process without a controlling console–in the background as an invisible (daemonized) process. This icon is not to be confused with management of the Firewall Server through the Windows Services interface. |
| | The **Uninstall** icon initiates the removal of the InJoy Firewall™ software product. |

| Sub-folder → Log Files | Icon Description |
|---|---|
|  | The **DHCPd Logs** icon starts the Log Viewer, pre-configured to show log files related to the DHCP server. |
| | The **IPSec Logs** icon starts the Log Viewer, pre-configured to show log files related to IPSec. |
| | The **PPPoE Logs** icon starts the Log Viewer, pre-configured to show log files related to PPPoE. |
| | The **PPTP Logs** icon starts the Log Viewer, pre-configured to show log files related to PPTP. |

| Sub-folder → Packet Tracing | Icon Description |
|---|---|
|  | The **Delete Trace File** icon deletes the file packet.trc. Use this command prior to new tracing sessions or to remove a previously recorded trace file. |
| | The **IP Trace (Start)** icon uses the sync.exe utility to enable a special firewall rule that logs all IP packets that reach the firewall to the file packet.trc in their raw (binary) format. |
| | The **IP Trace (Stop)** icon uses the sync.exe utility to remove the special packet logging firewall rule. The packet.trc file remains unmodified and can be used for investigative purposes. |
| | The **Format Trace (to Screen)** icon uses the included ipformat.exe utility to format all of the packets in packet.trc for display on the screen. To exploit the full potential of ipformat.exe, consider using it from the command line while redirecting output to a file. |

| Sub-folder → Tools | Icon Description |
|---|---|
|  | The **Kill Firewall** icon stops the Firewall Server by calling the sync.exe tool with the -kill option. |
| | The **Reload DHCP Configuration** icon activates changes to the DHCP Server configuration by calling the sync.exe tool with the -dhcpd option. |
| | **The Reload IPSec Configuration** icon activates changes to the IPSec VPN Plugin configuration by calling the sync.exe tool with the -ipsec option. |
| | The **Restart Firewall icon** activates changes to the Firewall Security Plugin by calling the sync.exe tool with the -firewall option. |

Note that you can reconstruct or recreate the InJoy Firewall™ desktop folder at any time by running the FOLDER script.

## 3.2. Starting the InJoy Firewall™ Server

To protect your network, **the InJoy Firewall™ Server must run continuously**. It is the only mandatory component of the InJoy Firewall™.

The simplest way to start the Firewall Server is to open the InJoy desktop folder and launch the InJoy Firewall™ Server application. This will cause a new console window to appear; the window will show output from the Firewall Server process.

To allow for customization, the Firewall Server can be started in several other ways:

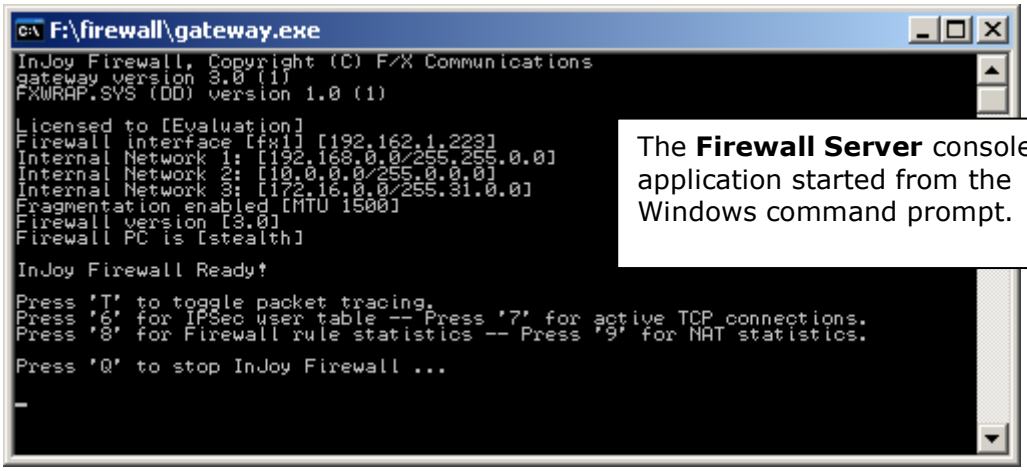
- At the **command prompt**
- As a **background process**
- As a **Windows service**

The following sections describe these options in detail.

## Starting the Firewall Server at the Command Prompt


The Firewall Server can be started at the command prompt on any supported Operating System. The command prompt is a process that allows you to enter operating system commands; examples include the Windows command prompt, OS/2 windows or terminal emulators such as xterm in Linux. From the command prompt, the Firewall Server is started like any other process—you enter its name:


As the Firewall Server runs, you will notice that it displays various kinds of output on the console, including the IP address of the interface being filtered and the address ranges of related internal networks.




The **Firewall Server** console application started from the Windows command prompt.

A number of keystrokes that can be used at any time are also displayed:

- 'T' to toggle packet tracing
- '6' to display the table of internal IPSec users
- '7' for active TCP connections
- '8' for firewall rule statistics
- '9' for NAT statistics
- 'Q' (case sensitive) to stop the firewall

As the firewall runs, additional operational information will be output to the console on an ongoing basis.

## Starting the Firewall Server in the Background

The background option allows the Firewall Server to run without a controlling console and was primarily designed for use with the OS/2 and UNIX based platforms. To execute the Firewall Server process in daemonized (invisible) fashion, add the -B argument to the command line:


When the Firewall Server is started in the background, there will be no console window containing server messages. To see these messages, you should either start the Firewall GUI or look in the file **logs\activity.log** file. Details on starting the Firewall GUI can be found in Section 3.3, "Starting the InJoy Firewall™ GUI."

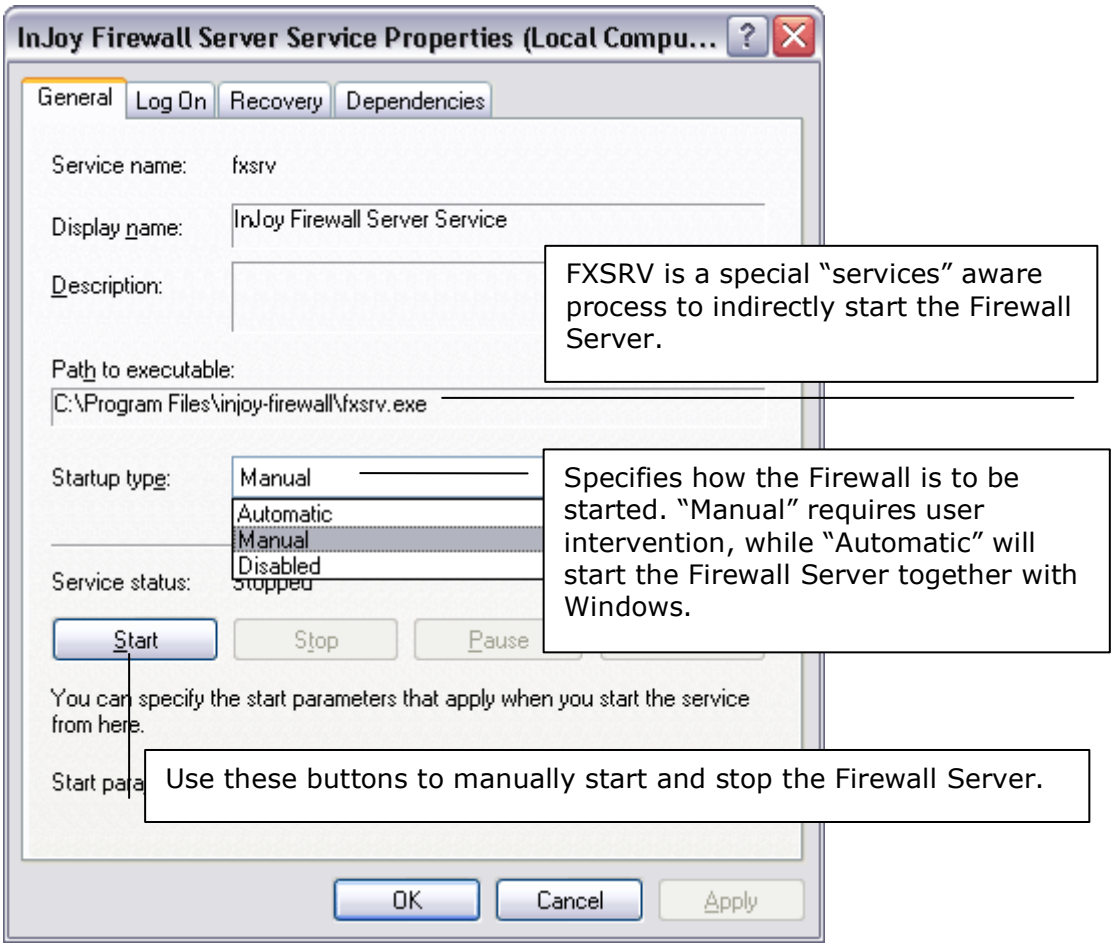
## Starting the Firewall Server as a Windows Service

If you plan to run the Firewall Server continuously, you may wish to set it up as a Windows service.

Windows services do not take up desktop space and do not require manual intervention in order to be started. When configured as a Windows service, the Firewall Server will be started together with Windows at boot time.

If you are using Windows, during installation you were given the option to start the Firewall Server as a Windows service. If you didn't choose to enable the Firewall Server as a Windows service at that time, you can configure the InJoy Firewall™ Server as a service now by following these steps:

1. Click on the Start menu and open the **Administrative Tools** submenu.
2. Click on the **Services** icon to launch the Services management tool.
3. Search for the **InJoy Firewall Server** service and double click on it.
4. Select the **Automatic** option from the **Startup Type** drop-down list.
5. Click on the **Ok** button to save your changes.




Once you have configured the InJoy Firewall™ Server as a Windows service, it is started automatically each time you start Windows.

## 3.3. Starting the InJoy Firewall™ GUI


The InJoy Firewall™ GUI is designed to provide a simple, yet powerful interface for management of the InJoy Firewall™. Because the Firewall GUI is an optional component, you can manually start and stop it on demand without affecting the performance of the Firewall Server.

**Note:** before you start the Firewall GUI, the Firewall Server should be running.

You can start the Firewall GUI from the:

- Desktop folder or Start Menu – like any other program.

- Command line – as shown below.

**To start the InJoy Firewall™ GUI from a command prompt**, enter the following command:


When you launch the Firewall GUI for the first time, a window with the default Firewall GUI appearance will be displayed:


By default, when you start the Firewall GUI without additional command line arguments or alternate settings, the Firewall GUI will connect to the Firewall Server running on the local machine. Using shared memory, the GUI will access the Firewall Server's configuration, statistics, and logs.

Once the InJoy Firewall™ GUI runs, you should perform a series of basic configuration steps necessary for successful firewall operation. These steps are discussed in detail in Section 4, "Basic Configuration."

## 3.4. Starting the InJoy Firewall™ Deskbar Application

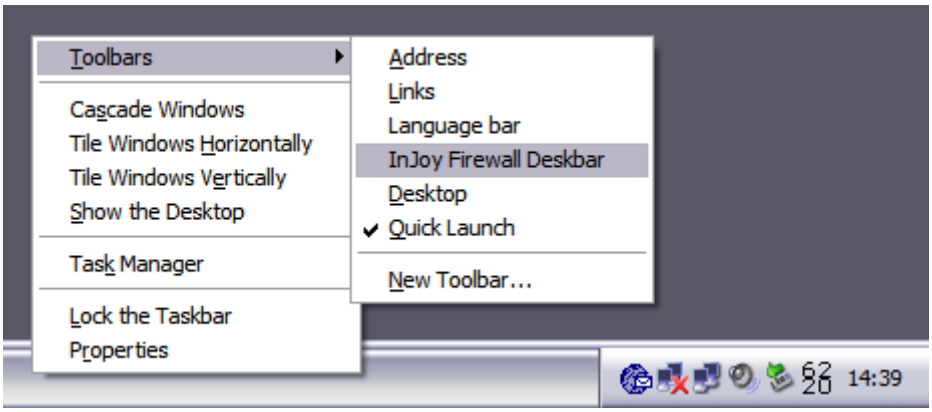
With the installation of the InJoy Firewall™ **on the Windows platform**, a small deskbar application is made available on your system.

The deskbar application empowers you to casually detect intrusion attempts and monitor network utilization, while preserving desktop space for other work.

### Enabling the Firewall Deskbar Application

To enable the deskbar application:

- With the mouse, right click the Windows taskbar
- Select the "InJoy Firewall Deskbar" in the "Toolbars" sub-menu.




If no local Firewall Server is running, a small "disconnected" icon is shown.

If a local Firewall Server is running, the Firewall Deskbar should immediately appear on the Windows taskbar - as shown below:

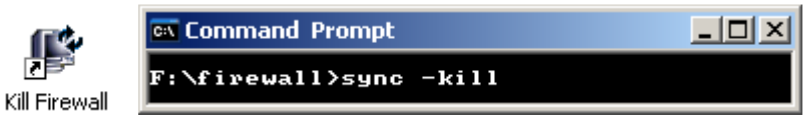

You can right click the Firewall Deskbar to easily configure appearance and Firewall Server relationship. For more information about the Firewall Deskbar please refer to Chapter 6.

## 3.5. Stopping the InJoy Firewall™

It may be necessary at times to stop the InJoy Firewall™ Server. In most cases, you can close the Firewall Server simply by closing the console window in which the Firewall Server is running. In certain cases, for example when the Firewall Server runs as a service or in the background, other methods for stopping the server may be more appropriate.

### Stopping a “Backgrounded” Firewall Server

If you started the Firewall Server as a background process, you can either stop it using the native process management features of the operating system in question or you can use the InJoy **sync** command:



The sync command can also be found in the "Tools" section of the InJoy desktop folder.

## Stopping the Firewall Server as a Windows Service

If you started the Firewall Server automatically as a Windows service, you can stop the Firewall Server by following these steps:

- Click on the Start menu and open the **Administrative Tools** submenu.
- Click on the **Services** icon to launch the Services management tool.
- Search for the **InJoy Firewall™ Server service** and double click on it.
- Click on the **Stop** button to stop the Firewall Server.

Note that even if you have stopped the Firewall Server using the Windows Services tool, it will start automatically again the next time you boot as long as automatic startup is selected.

## Stopping the Firewall Server Using the Firewall GUI

You can also stop the Firewall Server using the InJoy Firewall™ GUI; this option is discussed in Section 5.3, "Basic GUI Co."

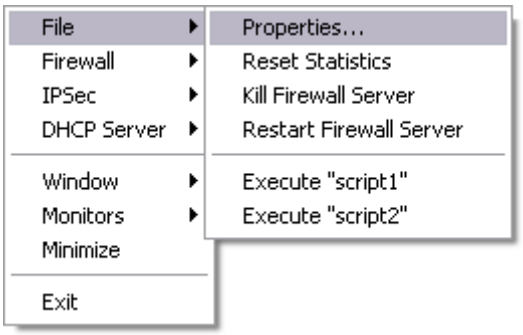
# 4 Basic Configuration

After you have started the Firewall™ Server, it is ready to protect you.

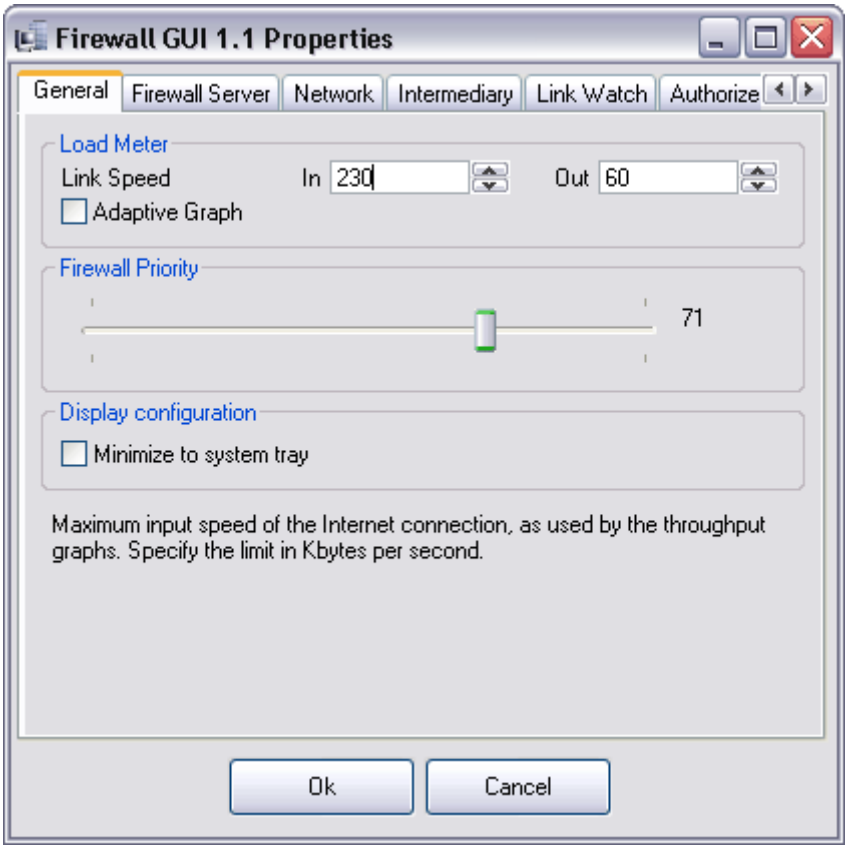
However, a few basic configuration steps are recommended to ensure that your firewall is properly configured and ready to deliver the operation you paid for?

| Step 1: | Step 2: | Step 3: | Step 4: |
|---|---|---|---|
| **Insert your License Key.**<br><br>This enables all the features you paid for. | **Verify the internal-net configuration.**<br><br>Required for the firewall to know which internal networks you have. | **Enable desired plugin features.**<br><br>To match your specific networking requirements. | **Check other properties and finish!**<br><br>To ensure the defaults match your needs and to activate your changes. |

All of the configuration steps in this section are performed using the Firewall Properties dialog. To open the Firewall Properties dialog now, start the InJoy Firewall™ GUI and right-click the vertical grey area on the left side of the GUI.



As the pop-up menu appears, select "**File | Properties"** and wait for the dialog to appear – as shown below.

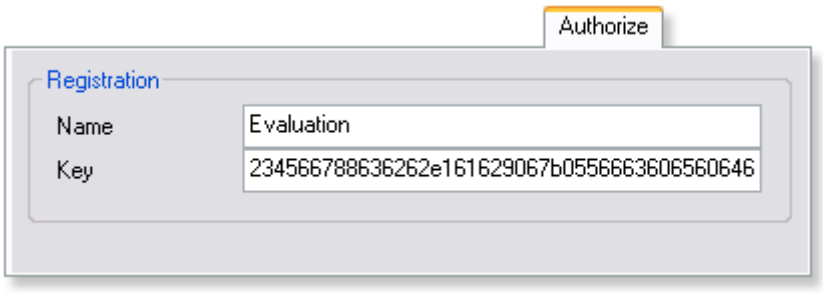



## 4.1. Inserting the License Key

Before configuring any other aspects of your InJoy Firewall™, you should insert the License Key that you received with your purchase.

To insert your License Number, click on the **Authorize** tab. Enter the name under which you purchased InJoy Firewall™ into the **Name** box, then enter the License Key you were given into the **Key** box.

Both the Name and the Key must be entered **exactly** as you received them, without trailing spaces and in the same case. We recommend using the clipboard copy&paste function for this operation.

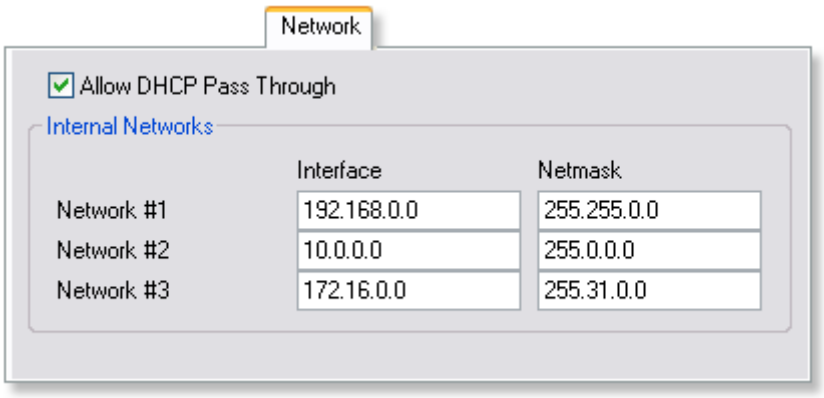



**Upon successful registration**, you will NOT see a success message, but you will be prompted to restart the Firewall Server. Hereafter the features you paid for will be available.

If you **do not have a License Key**, you will see the word "Evaluation" in the Name box and an automatically generated evaluation license key in the Key box. This indicates that InJoy Firewall™ is operating in evaluation mode for testing purposes.

## 4.2. Verifying Internal Network Configuration

To operate correctly, the InJoy Firewall™ must have address information that accurately reflects the topology of your internal network(s) – if any. To view the default settings, click on the **Network tab** in the Firewall Properties dialog.




**DHCP Pass Through**
The DHCP Pass Through is a *convenience* feature to allow Dynamic Host Configuration Protocol (DHCP) transactions to take place transparently through your firewall – without the need for firewall rule creation. Enable if your Firewall PC obtains its IP address automatically from a DHCP server.

**Internal Networks**
It is essential that you compare the network settings stored by the InJoy Firewall™ to the IP address ranges that your internal network(s) use.

By default, these IP address ranges include the addresses reserved for internal use under RFC 1918. You should however ensure that IP ranges assigned to you by your Internet Service Provider (ISP) and address ranges used by your Virtual Private Network (VPN) are also included. You can enter up to three networks and matching network mask values into the Interface and Netmask boxes.

The default settings for the three networks that can be configured in this tab are the networks reserved for internal use under RFC 1918:

- 192.168.0.0, network mask of 255.255.0.0
- 10.0.0.0, network mask of 255.0.0.0
- 172.16.0.0, network mask of 255.31.0.0

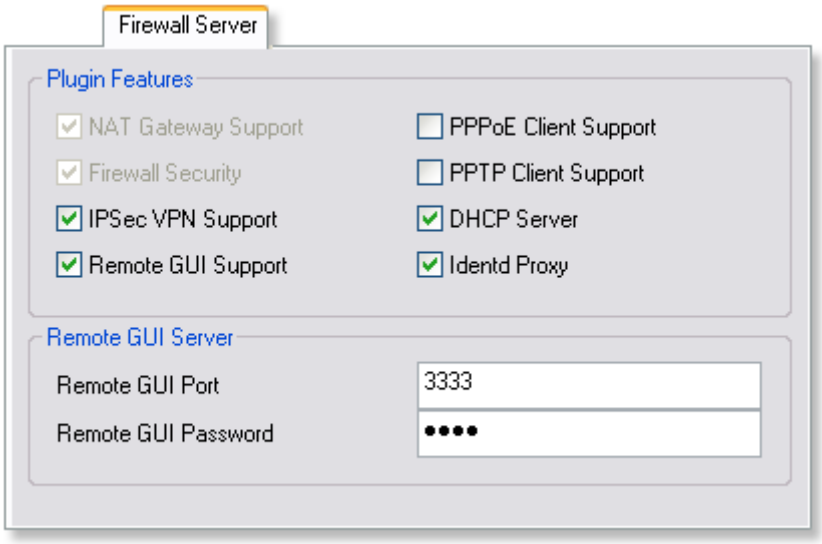
Though these values are common, they do not necessarily reflect those in use by your network(s); be sure to enter the correct values before continuing.

**Note:** to configure more than 3 internal networks (you may enter up to 7), refer to the file **config\gateway.cnf**. The applicable configuration attributes are *Internal-Net-1* through *Internal-Net-7*, and *Internal-Netmask-1* through *Internal-Netmask-7*. To disable an internal net, set it to "0.0.0.0".

## 4.3. Selecting Plugin Features

Because the InJoy Firewall™ is modular, you can alter its behavior by enabling or disabling Plugin Features—software modules which provide a particular service or capability. Before using your firewall, you should be sure to enable any Plugin Features whose functionality you plan to use; you should also be sure to disable Plugin Features that provide functionality you won't use.

To access the list of Plugin Features available to InJoy Firewall™ users, click on the **Firewall Server** tab of the Firewall Properties dialog. After clicking the tab, you will see a list of feature checkboxes corresponding to the Plugin Features available. To enable a Plugin Feature, check its box. To disable a Plugin Feature, uncheck its box.




**The Plugin Features are:**

- **NAT Gateway Support**, which enables Network Address Translation (NAT) between interfaces, allowing your firewall to act as a router or gateway for other machines on your network(s). You cannot disable the NAT Plugin.
- **Firewall Security**, which enables advanced firewall and packet filtering features for enhanced security. You cannot disable the Firewall Security Plugin.
- **IPSec VPN Support**, which enables the InJoy Firewall's IPSec/IKE implementation for Virtual Private Networks (VPNs).
- **Remote GUI Support**, which enables remote administration of the InJoy Firewall™ Server using the InJoy Firewall™ GUI.
- **PPPoE Client Support**, which allows InJoy Firewall™ to support Point-to-Point Protocol over Ethernet (PPPoE) clients.
- **PPTP Client Support**, which allows InJoy Firewall™ to support Point-to-Point Tunneling Protocol clients for Virtual Private Networks (VPNs).
- **DHCP Server**, which allows InJoy Firewall™ to listen for and answer Dynamic Host Configuration Protocol (DHCP) requests.

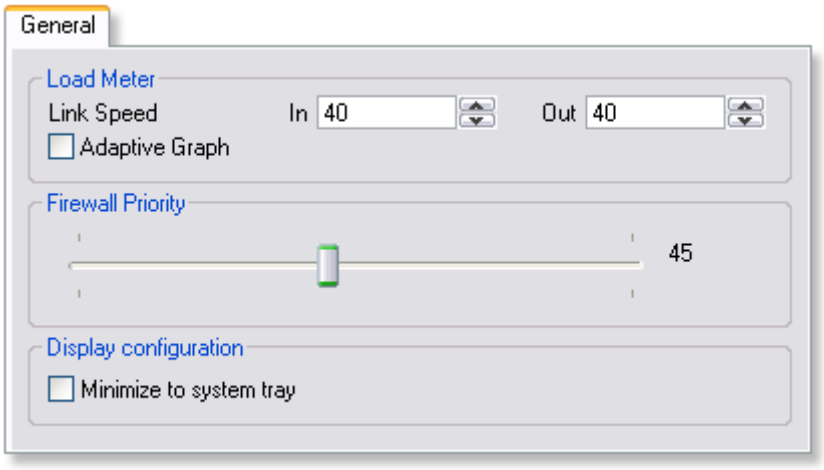
- **Identd Proxy**, allows identification requests using RFC 1413 to be forwarded through your firewall to an internal Identd server – such as those built into IRC chat clients.

Additional documentation for the major InJoy Firewall™ plugin features, such as the IPSec and Firewall Security plugin, is available in separate documents.

## 4.4. Other Firewall Properties

Other configuration options in the Firewall Properties dialog may also be important - however not critical - for your use of the software. Follow the steps below to verify or change any of the default settings.

### General Options




**Load Meter**
InJoy Firewall™ allows you to monitor your network traffic with a bandwidth load meter. To ensure the accuracy of the meter's display, follow these steps:

1. Click on the **General** tab in the Firewall Properties dialog.
2. Enter the speed of your link for incoming traffic, in kilobytes per second, into the **In** box.
3. Enter the downstream speed of your link for outbound traffic, in kilobytes per second, into the **Out** box.
4. If you want the load meter line-graph to auto-scale, based on the previous peek performance, check the **Adaptive Graph** box.

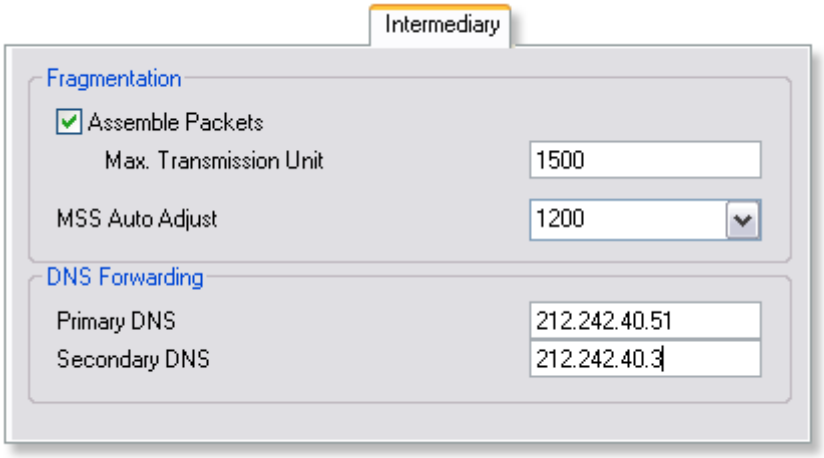
**Firewall Priority**
The InJoy Firewall™ allows you to adjust the priority of the Firewall Server process. In general, the default priority is the recommended setting. However, if you wish to change the process priority, follow these steps:

1. Click on the **General** tab in the Firewall Properties dialog.
2. Adjust the **Firewall Priority slider** up or down, depending on whether you want to raise or lower the priority of the Firewall Server process.

Changing the Firewall priority may be critical when the PC is used for multiple purposes or when top-performance is of the highest importance.

**Minimize to system tray**
Enable this option for the Firewall GUI to minimize to the system tray, rather than the taskbar - on the Windows platform.

## Intermediary




**Fragmentation Control**
Fragmentation Control allows you to adjust the Maximum Transfer Unit (MTU) and Maximum Segment Size (MSS) values for traffic passing through your firewall. To edit these values, follow these steps:

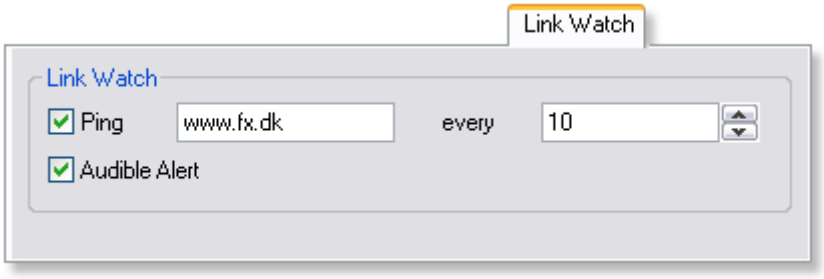
1. Click on the **Intermediary** tab in the Firewall Properties dialog.
2. Enter a Maximum Segment Size value in the **MSS Auto Adjust** box (1200 is recommended). To disable MSS and allow the TCP/IP stack to set the MSS value, select **Disable** from the drop-down list.
3. To allow your firewall to reassemble and analyze fragmented packets (recommended), check the **Assemble Packets box**, then enter an MTU value in the **Max. Transmission Unit** box (1500 is recommended).

If you plan to use IPSec tunneling, PPPoE or PPTP, the MTU and MSS values are of outmost importance. Please refer to the relevant documents for further information.

**DNS Forwarding**
Domain Name System (DNS) request forwarding allows DNS requests from the internal network to be forwarded to any domain name servers that you specify. If DNS Forwarding values are set, any DNS request sent to host 1.1.1.1 and 1.1.1.2 from your internal networks are forwarded to the hosts supplied here.

If you receive DNS Server addresses dynamically through a PPPoE link, it is recommended that you enter either static DNS Server addresses (which are always valid) or disable the use of this feature.

### Link Watch



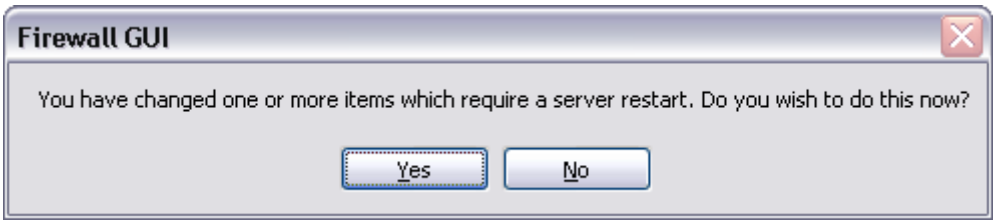

Link Watch allows your firewall to regularly ping another host in order to monitor the integrity of your data link. To enable Link Watch, follow these steps:

1. Click on the **Link Watch** tab in the Firewall Properties dialog.
2. Check the **Ping** box and enter the name or IP address of the host you wish to regularly ping.
3. Enter a delay (in seconds) between pings in the **every** box.
4. If you want to hear an audible alarm every time the link goes down, check **Audible Alert** box.

## 4.5. Finishing the Configuration

Having completed the InJoy Firewall™ properties configuration, you are ready to click **OK** to save and activate the changes.

Depending on the changes made, the Firewall Server may need to be restarted. If restarting is required, you will see the following message:




Click **Yes** to automatically restart the InJoy Firewall™ Server.

**Congratulations!**
At this point, you have completed the basic configuration and the InJoy Firewall™ is ready to share your network connection and protect your resources.

**To optionally verify the default Security Level, please refer to section 8.3, for more information.**

It is also recommended that you consult section 7 for more information about the InJoy configuration options and default values.

# Part II
# Graphical Administration

# 5 The User Interface

The cross platform interoperable Graphical User Interface (GUI) offers Firewall Server configuration support, customizable real-time traffic monitoring, statistics, link watching and remote management. It includes configuration support for PPPoE, IPSec, DHCP Serving, Traffic Shaping, Firewall security and much more. Text mode only operation is provided for older RAM starved machines.

This section discusses the major features of the InJoy Firewall™ GUI:

- Security and usability.
- Look and Feel options, including the ability to change themes, colors, and fonts and to save these changes as GUI profiles.
- Basic GUI commands that can be used to change the status of the Firewall Server.
- Statistics and Information Monitors that show the status of the Firewall Server and track traffic.
- Firewall Monitors, which allow the administrator to monitor the activity of the firewall plugin, including such things as rule match counts.
- Remote firewall administration using the Firewall GUI.
- Management of multiple local Firewall Servers using the Firewall GUI.

For details on how to launch the InJoy Firewall™ GUI, refer to Section 3.3, "Starting the InJoy Firewall™ GUI."

## 5.1. Introducing the Firewall GUI


The InJoy Firewall's Graphical User Interface (GUI) is an optional tool that provides a powerful interface for managing InJoy Firewall Servers.

Multiple instances of the GUI can run simultaneously; each of these can connect to Firewall Servers either locally or remotely, greatly simplifying administration tasks.

Because the GUI is optional, it can be started and stopped on demand.

### Firewall GUI Security

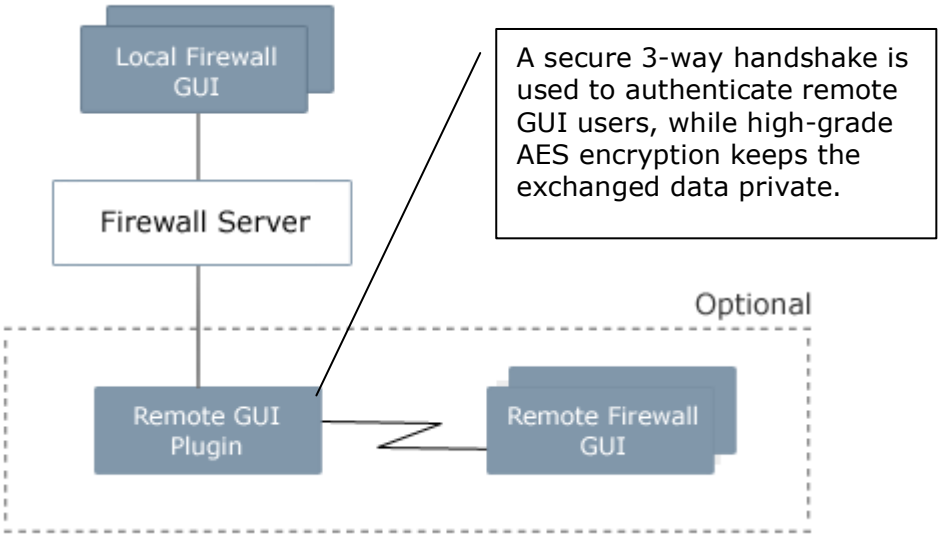
To meet government and enterprise-grade security requirements, the Firewall Server's GUI access has been specifically hardened against attacks that could compromise the security of your network.

This has been done through a number of measures:

- **Local GUI Connections use Shared Memory**
  Local GUI management of Firewall Server is possible without loading the Remote GUI Support and without opening any TCP/IP ports.

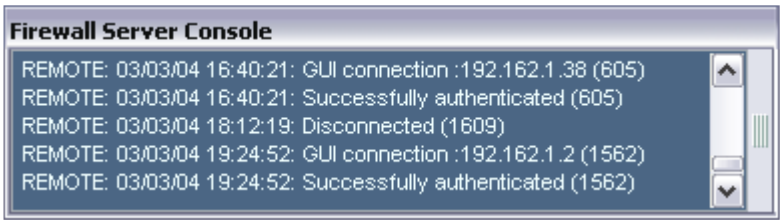
Local GUI connections use shared memory requiring each participating process to have physical access to the computer's memory in order to manage the Firewall Server. This allows administrators to do local GUI management of the Firewall while preventing remote management.

- **Remote GUI Support as a Separate Plugin**
  The remote management has been designed as a separate Firewall Server plugin that needs to be specifically enabled to allow remote GUI connections. Users concerned about security risks associated with remote GUI administration can disable this functionality – thereby completely preventing the Remote GUI code from being loaded.
- **Strong Authentication and Encryption**
  The Remote GUI uses an encrypted 3-way handshake to authenticate remove users.
- **Strong Encryption**
  High-grade AES (Advanced Encryption Security) is used to protect the data transmitted over the GUI connection.




- **Limiting Remote GUI Access**
  Just like all other TCP connections, the InJoy Firewall™ GUI connections adhere to the overall Firewall policy. Administrators can create standard Firewall rules to easily configure which remote IP addresses that are allowed to access the Firewall Server GUI port (3333 by default) and thus further limit exposure of the remote GUI feature.
- **GUI Hackers are Logged and Blacklisted**
  The InJoy Firewall™ ships with rules that automatically Log a Security Alert and/or Blacklist Remote GUI users that attempt to login with incorrect passwords (3 times within an hour). Logging of such attempts starts on Security Level-5 and Blacklisting starts at Security Level-6.
- **Remote GUI Operations Logged**

As a precautionary measure, when the Firewall GUI connects to (or disconnects) from a remote Firewall Server, the Firewall Server will make note of the activity - on its console monitor:




Major Remote GUI operations are also logged to the **firewall.log** file, allowing administrators to easily maintain an overview of past GUI use. In addition, the location of the **firewall.log** file can be specified to be a network drive, allowing the administrator to further set up and customize specialized GUI activity monitoring.

Local GUI connections are not reported on the server console.

## Performance

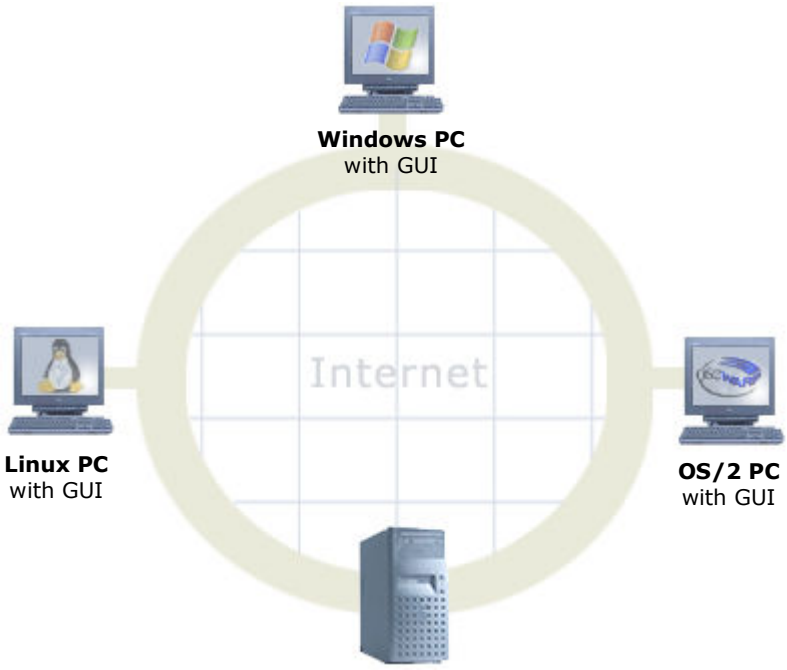
To ensure maximum performance and flexibility, the Firewall GUI is delivered as a standard Windows/Linux/OS2 application, compiled natively for each supported OS platform.

Local GUI connections use shared memory, enabling it to perform just as fast as if it had been an integral part of the InJoy Firewall Server.

Compression and optimization algorithms ensure that Remote GUI connections require minimum bandwidth and guarantee that only changed data is actually sent over the TCP connection.

### A Native GUI for Every OS Platform

Because the GUI uses one configuration file format and has a similar appearance across all InJoy platforms, administrators can manage multiple-platform networks without needing to become familiar with a new tool for each OS platform.



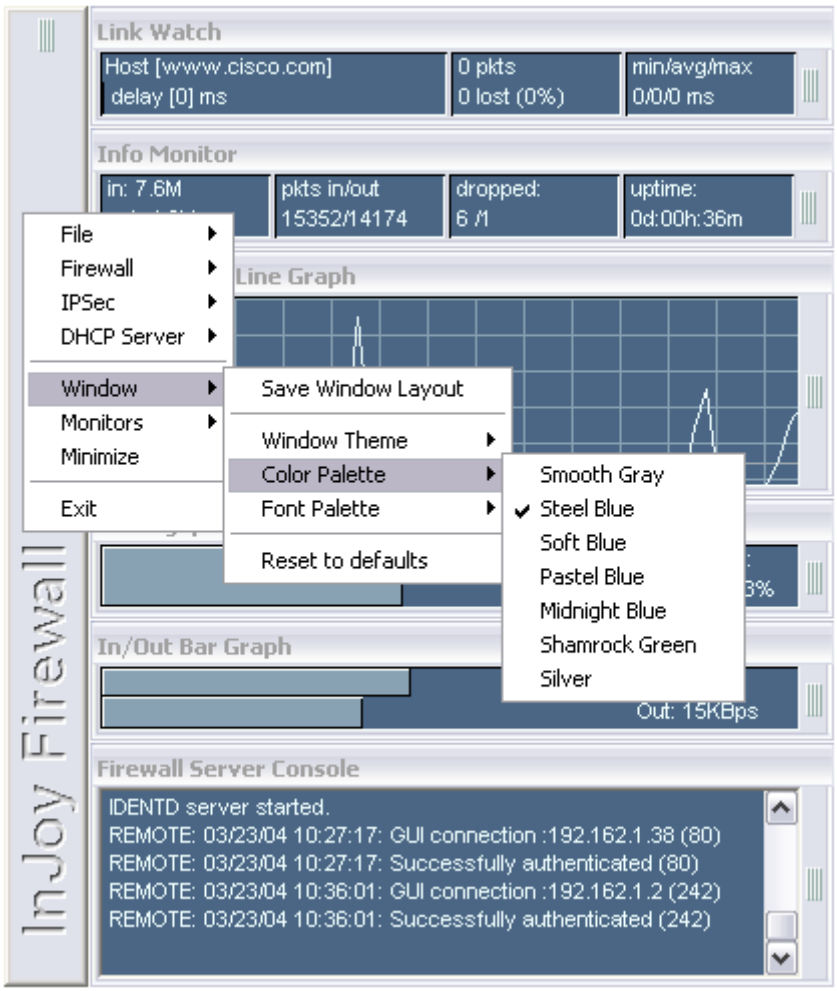

**Remote Firewall Server**

For instance, a Firewall GUI running on Windows can manage a remote Firewall Server that runs on Linux.

## 5.2. Managing the GUI Look and Feel

The appearance of the InJoy Firewall™ GUI is highly configurable. Network administrators can tailor the appearance of the GUI to suit their own (or the customer's) unique computing environment and needs. Once the desired appearance has been achieved, the GUI's appearance settings can be saved. Multiple preference files can be saved; this allows users of multiple Firewall Servers to use a unique appearance profile for each instance of the Firewall GUI.

To access the appearance options for the Firewall GUI, right-click in the vertical gray dock area and select **Window** to display a list of submenus.




- The Window **Theme** submenu allows you to select from a number of visually appealing organizational themes.
- The **Color Palette** submenu allows you to select from a number of predefined color schemes.
- The **Font Palette** submenu allows you to display the text of the Firewall GUI in one of several fonts.

## Choosing a GUI Theme

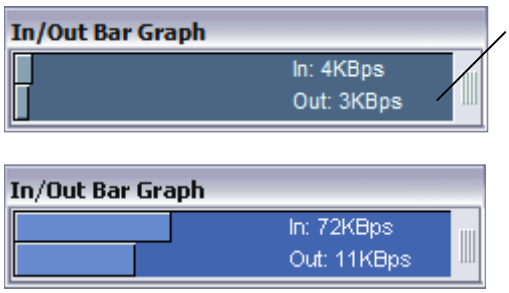
Themes provide the user with a way to alter the layout appearance of the Firewall GUI and the amount of information it displays by default. Available themes include, but are not limited to:

- The **Micro** theme, which displays Firewall Server bandwidth usage using a minimum of desktop area.
- The **Default** theme, which is the default appearance of the Firewall GUI.
- The **Enterprise Server** theme, which displays additional statistical and status information about the Firewall but also uses a larger amount of desktop area.

More themes exist to match your requirements and taste.

## Color and Font Palettes

Because computer displays, lighting conditions and personal preferences vary, the Firewall GUI allows you to apply one of several different color and font palettes to the GUI's windows.




Font and color palettes are often used as visual cues for differentiating between GUI instances when multiple firewalls and Firewall GUIs are running.

The selection of available font palettes varies between platforms.

To apply a particular font or color palette to your GUI window, simply select the palette you wish to use from the **Color Palette** or **Font Palette** submenus.

## Saving Appearance Preferences

Once you have configured your theme, color, and font palettes to suit your needs, you can save the appearance preferences of your Firewall GUI. Once this has been done, each time you start the Firewall GUI it will take on the appearance you have chosen.

To save your appearance preferences, right-click in the vertical gray area on the GUI dock window. When the pop-up menu appears, select Window and then "Save Window Layout". This will cause the following appearance preferences to be saved:

- The position of the GUI and monitors on your display
- The color and font palette you have chosen for this GUI
- The list of visible monitor windows

## Restoring Default Appearance

After changing the appearance of the Firewall GUI and saving your changes, you may find at some point that you wish to restore the default color, theme and monitor appearance of the Firewall GUI. To restore the default appearance of the Firewall GUI:

- Right-click in the vertical gray area of the GUI dock window. When the pop-up menu appears, select **"Window | Reset to defaults"**.

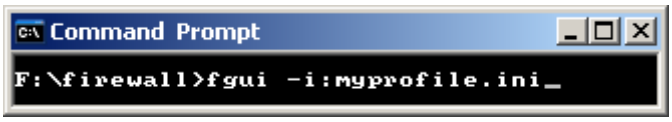
The GUI settings are stored in the file my-themes.ini. By deleting this file, you can also restore default GUI operation.

## Using Multiple Preference Files

By default, the Firewall GUI will store its entire appearance profile in the text file called fgui.ini. With the exception of font selections, this file is portable across all InJoy platforms.

Under some circumstances, it can be helpful to maintain alternate appearance profiles for the Firewall GUI. This is often the case when multiple instances of the Firewall GUI will be running on the same display.

If desired, the Firewall GUI can be instructed to use an alternate file to control its appearance by starting the Firewall GUI from the command prompt and supplying the **-i** option. For example, the following command would start the Firewall GUI using an appearance profile called myprofile.ini:



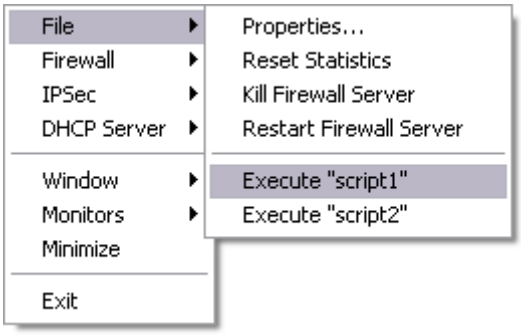

After starting the Firewall GUI using the **–**i option, any appearance changes you save will be stored in the alternate configuration file, rather than in the default configuration file. Note that if you launch the Firewall GUI and specify a nonexistent profile name, a new file will be created for you using the default Firewall GUI appearance.

## 5.3. Basic GUI Commands

The Firewall GUI provides a set of simple commands to alter the running state of the Firewall Server. These commands include:

- **Reset Statistics**, which can be used to reset to zero all of the statistical counters maintained by the Firewall Server.
- **Kill Firewall Server**, which can be used to stop the Firewall Server.
- **Restart Firewall Server**, which can be used to stop and then restart the Firewall Server.
- **Execute "Script 1" / "Script 2"**, which can be used to trigger execution of two pre-defined scripts. By putting your own commands into these script files at the Firewall Server location, you can use the GUI to remotely start e.g. a telnet or ftp server, enable packet tracing, or install new software. On OS/2 and Windows, the scripts are named script1.cmd and script2.cmd. On Linux, the file extension is ".sh" (instead of ".cmd").

To access the GUI commands, right-click in the vertical gray area on GUI dock window. When the pop-up menu appears, select **File** to display the submenu containing the list of available controls. Then, choose the task that you would like the Firewall Server to carry out.

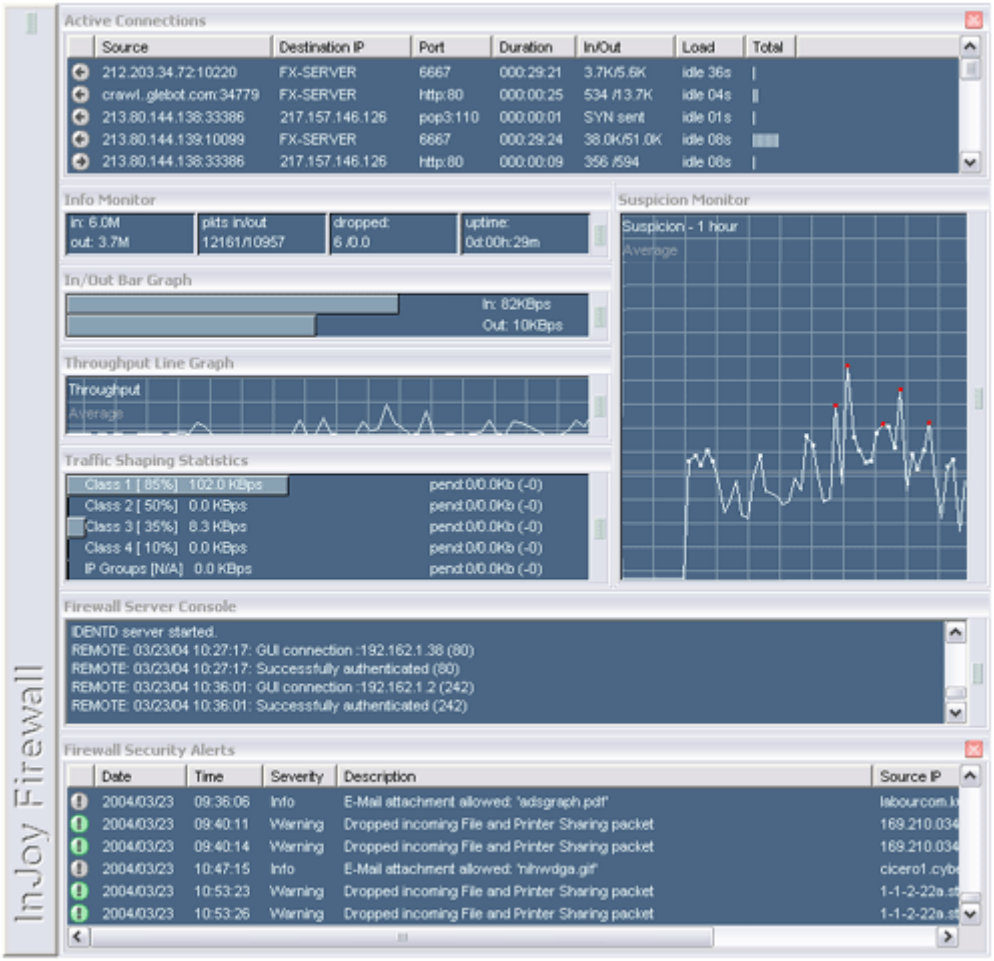



*Note: Stopping or restarting your Firewall Server can interrupt users' open network connections. When you installed InJoy Firewall™, you were asked whether you wished to ALLOW or BLOCK all IP traffic when the Firewall Server isn't running. If you chose to ALLOW all IP traffic when the Firewall Server*

*isn't running, killing the Firewall Server will have a negative impact on network security.*

## 5.4. Basic Statistics and Information Monitors

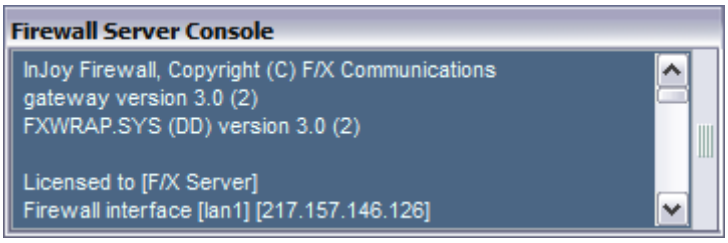
The InJoy Firewall™ GUI provides a number of statistics and information monitors designed to provide general status information about the running Firewall Server.




To toggle the display of a particular monitor on or off, bring up the pop-up menu and select **Monitors**. Then, choose the statistics and information monitor that you would like to display or hide from the top half of the list.

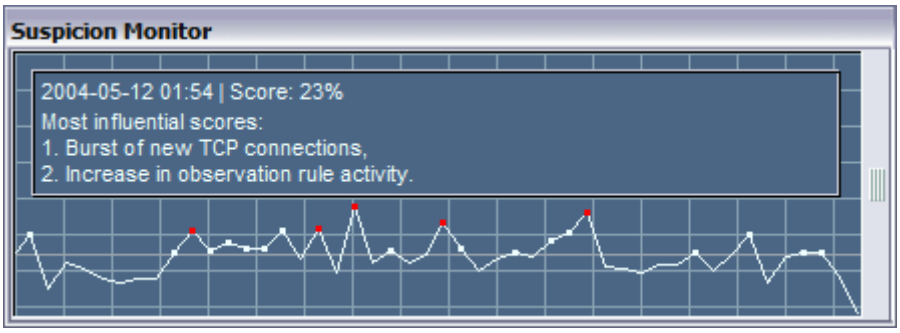
## Firewall Server Console

The Firewall Server Console displays operation-related messages from the Firewall Server. These messages are the same messages that can be seen on the console in which the Firewall Server is running; they may be related to starting and stopping the firewall, configuration changes, network interfaces, interface errors, or other operational details.



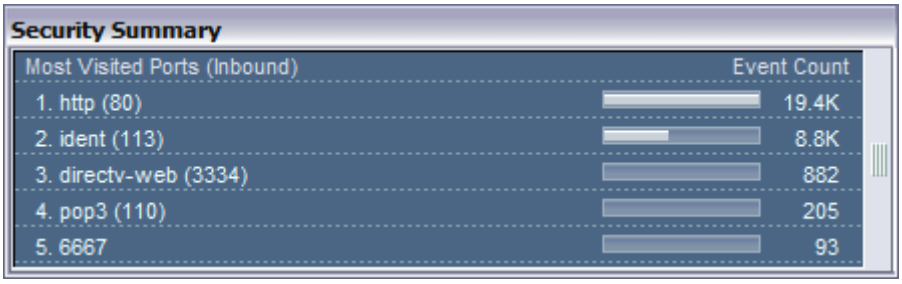

## Suspicion Monitor

The Suspicion Monitor provides an ongoing visual representation of intrusion activity. The Firewall calculates a score each minute, based on factors such as the number of dynamic firewall rule created, number of new tcp connections, alerts logged, packets dropped, and more. Five peaks are marked red to indicate the most noticeable activity (possible attacks). The mouse pointer can be placed on top of these peaks to get a description of the offending activity, including the most influential scores and a time-stamp. Right clicking the monitor allows you to toggle between 1-hour or 24-hour representation of the attack history.



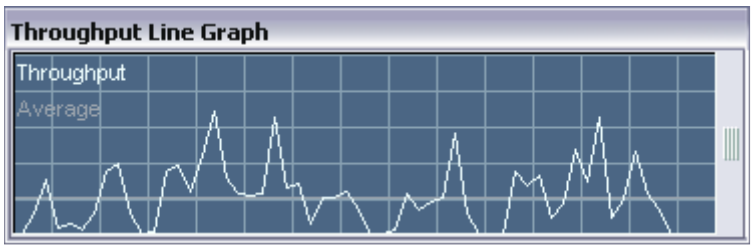

## Security Summary

The security summary is a looping monitor that keeps track of high-scores when it comes to most blocked ports and IP addresses. On the left side of the monitor you see the port or IP address, and in the right side of the monitor you see the event count. The port http (80) and an event count of 19.4K would indicate that 19400 incoming web connections have been recorded. You can click the Security Summary monitor at any time to instantly skip to its next page. Right clicking the monitor presents a number of options, allowing you to stop the cycling and e.g. focus on a single page of information.



## Throughput Line Graph

The Throughput Line Graph monitor provides an ongoing visual representation of your network's throughput over time. The average throughput for the currently displayed time period is shown as a free-floating horizontal line.




## Throughput and In/Out Bar Graphs

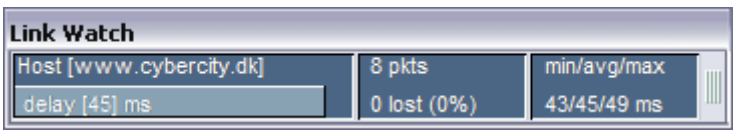
The Throughput Bar Graphs provide an instantaneous visual representation of your network's throughput. Current in/out throughput is displayed as a numeric value on the right side of the monitor and as a bar-graph on the left. The scale used by the throughput graphs depends on the **Load Meter** preferences in the Firewall Properties dialog, as described in Section 4.4, "Other Firewall Properties."



## Link Watch

The Link Watch monitor displays the last reported status of the connection to the Link Watch host. The host can be specified in the **Link Watch** preferences in the Firewall Properties dialog, as described in Section 4.4, "Other Firewall Properties." The monitor contains three sub-panels, each of which provides information about communication with the Link Watch host:

- The leftmost sub-panel displays the name or IP address of the Link Watch host, a number which indicates the ping response delay, and a horizontal bar graph to represent this delay visually.
- The centre sub-panel shows the number of packets which have been sent to the Link Watch host, the number of packets which have received no response in return, and the overall percentage of packets lost.
- The rightmost sub-panel shows the minimum, average, and maximum return times for ping responses.



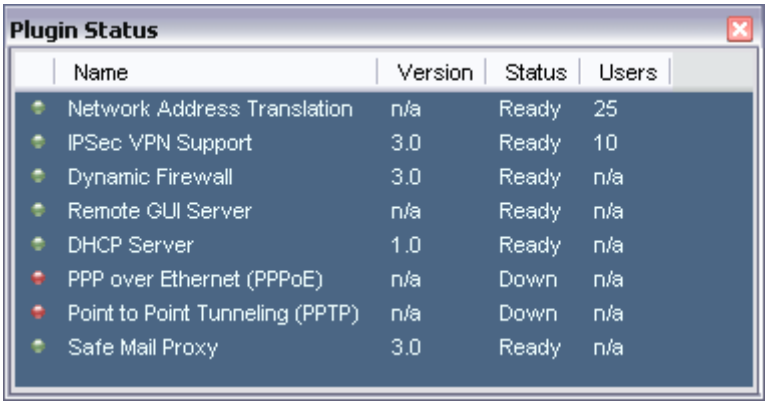
## Information Monitor

The Information Monitor contains four sub-panels, each of which displays a variety of statistical information about the running Firewall server:

- The first (leftmost) sub-panel shows the total amount of data sent and received on the firewalled network interface since the Firewall Server was started.
- The second sub-panel shows the number of packets which have been sent and received since the Firewall Server was started (in / out).
- The third sub-panel shows the number of packets which have been dropped since the Firewall Server was started (in / out).
- The fourth (rightmost) sub-panel shows the amount of continuous running time which has elapsed since the Firewall Server was started.


## Plugin Status

The Plugin Status monitor shows the current status of the Firewall Server plugins. The display provides information about the individual plugins, their version, their operational status and the number of users the plugin, is registered for – if available.

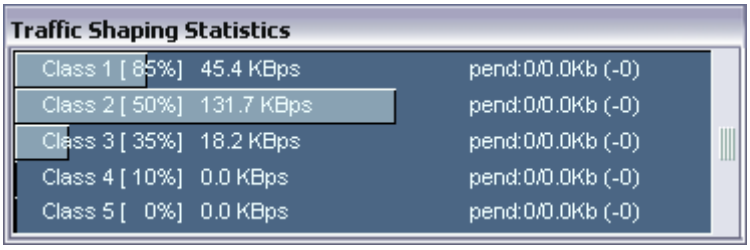



## Traffic Shaping Statistics

The Traffic Shaping Statistics monitor shows the way the Firewall Server distributes traffic between the different traffic priority classes.

The graphs are by default organized so Class #1 represents high priority traffic (85% priority), while Class #4 is for low priority traffic (10% priority). On the right side of the monitor the pending traffic is displayed, together with the number of packets that were discarded due to exhausted queues – this value is represented as (-0). Class #5 is a special traffic class, representing the amount of traffic that is limited by rule or per IP address.

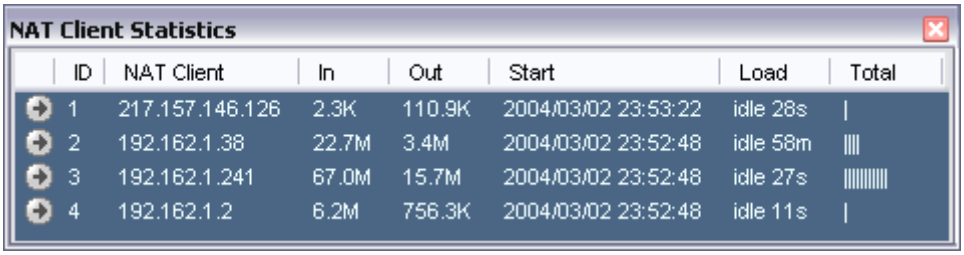
The horizontal scale used by the bar in the graph depends on the **Traffic shaping Statistics** preferences in the Firewall Properties dialog, as described in Section 4.4, ”Other Firewall Properties.”




## NAT Client Statistics

The NAT Client Statistics monitor displays information about the Network Address Translation (NAT) clients on your network. The table will record all the internal work-stations that use the InJoy Firewall™ Server as a gateway for Internet access. The display provides several columns of information; these columns include:

- The ID column, which shows the instance number of the NAT client. ID 1 is reserved for the Firewall Server IP address itself.
- The NAT Client column, which shows the IP address of the internal work-station recorded in the NAT table.
- The In and Out columns, which show the accumulated amount of inbound and outbound traffic, respectively, for the NAT Client in question.
- The Start and Load columns, which show the time at which the NAT Client first used NAT and the amount of time which has elapsed since its last use of NAT.
- The Total column shows the current traffic load of the work-station, visually.



# 5.5. Advanced Firewall GUI Monitors

The Firewall GUI includes a series of monitors designed to allow the administrator to observe the running status of the firewall and its various security capabilities and components.

This section provides just a brief introduction to the predefined Firewall GUI Monitors. For a more detailed explanation of how to fully exploit these monitors, please see the "Firewall Security Guide".

## Firewall Monitor Information Fields

A number of separate firewall monitors are discussed in the next section. The monitors report activity using a selection of fields from the following list:

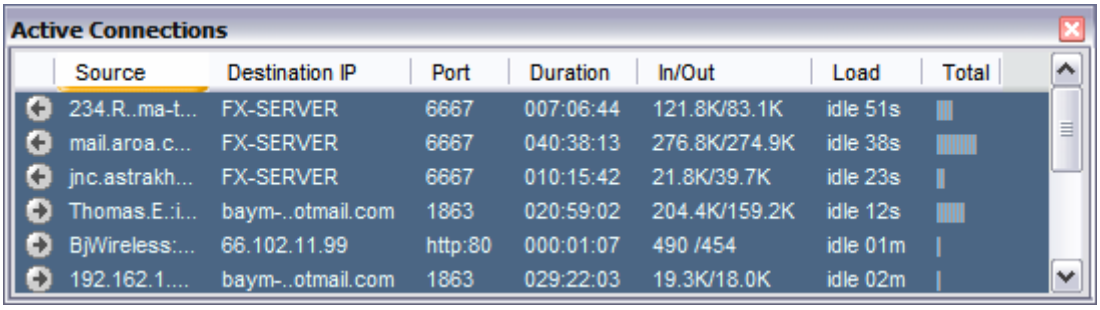
- Source IP and Destination IP show the IP address of the host from which the monitored event originated or was intended, respectively.
- Source Port and Destination Port show the network port (TCP or UDP) from which the monitored event originated or was intended, respectively.
- State shows the state of TCP connections, either "SYN_SENT" for a connection requested or "Established" for an open connection.
- Duration shows the length of time represented by the monitored event.
- Idle shows the amount of time the monitored even (e.g. a TCP connection) has been idle - i.e. no network traffic observed.
- In/Out shows the number of bytes, kilobytes, megabytes or gigabytes which have arrived or which have been sent from the network interface in question.
- Date shows the date on which the monitored event occurred.
- Time shows the time at which the monitored event occurred.
- Severity shows the seriousness or severity of the monitored event, one of Info, Warning, Low, Medium, High, or Major.
- Direction shows the direction of the monitored event, either inbound (originating in the external network) or outbound (originating in the internal network).
- Protocol shows the transport layer protocol (i.e. TCP, UDP, ICMP, or other protocols) that was employed by the monitored event.
- URL Request shows the URL which was requested by the originating host when an HTTP request is logged.
- Description shows a brief description of the monitored event.

## Firewall Security and Traffic Monitors

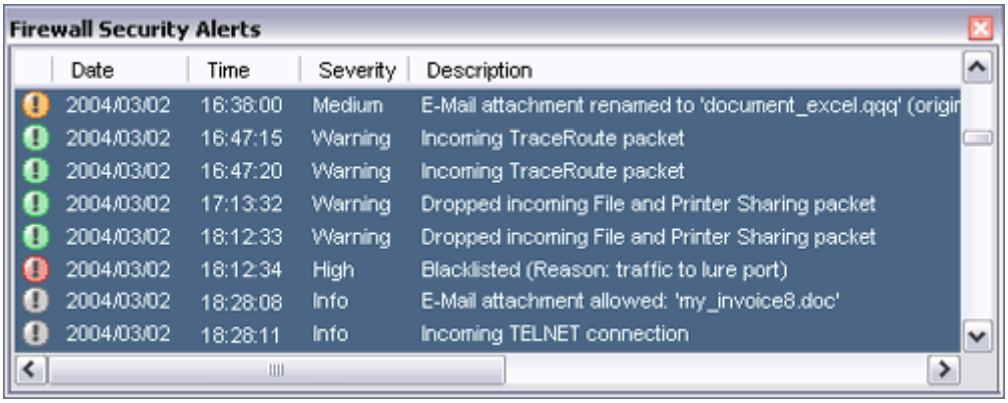
The following operations can be monitored using the Firewall monitors.

**Active Connections**
The Active Connections monitors the TCP connections which are currently opened through the firewall network interface. Each line denotes an active TCP connection and an icon to the left indicates the direction of the connection. If the icon points to the left, it's an inbound connection (from the Internet to you). All other connections are outbound (from inside your firewall protected network, to the Internet). To the right, the Total column allows you

to see just how much bandwidth a single connection has consumed in relation to the other active connections.




**Security Alerts**
The Security Alerts monitors traffic for potential security issues and displays a warning level for each potential problem event. You can click the alerts to get more information, including a longer description and a [formatted/hex] dump of the offending IP packet (if any).




**Rejected Connections**
Rejected Connections monitors the connection attempts to the firewall network interface which have been rejected by the Firewall Server due to matched firewall rules, blacklisting or other security threats.

**Connection Log**
The Connection Log monitors the successful connections which have been opened in the past on the firewall network interface.

**Dropped Packets**
Dropped Packets monitors packets which have been dropped by the Firewall Server as a result of the active set of firewall rules or other security violations.

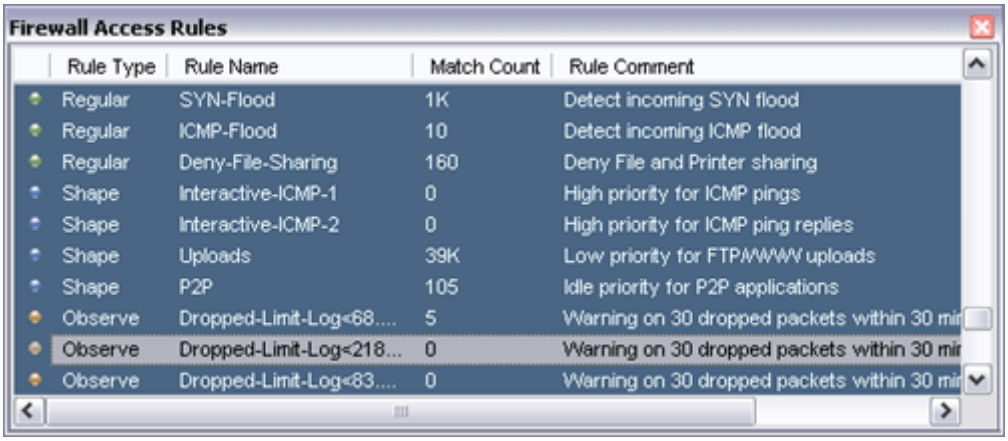
**Blacklisting**
Blacklisting monitors the list of hosts which have been blacklisted (blocked) after violating the Firewall rules.

**HTTP Requests**
HTTP Requests monitors the HTTP requests which have passed through the InJoy Firewall™.

**Firewall Access Rules Monitor**
A special firewall monitor called Access Rules displays the list of rules that are active for the currently running Firewall Server. There are several different types of rules which might appear in the Access Rules monitor:

- Regular filtering rules, represented by a green icon
- Traffic Shaping rules, represented also by a green icon
- Blacklisting rules, represented by a red icon
- Observation rules, represented by a yellow icon containing an exclamation mark

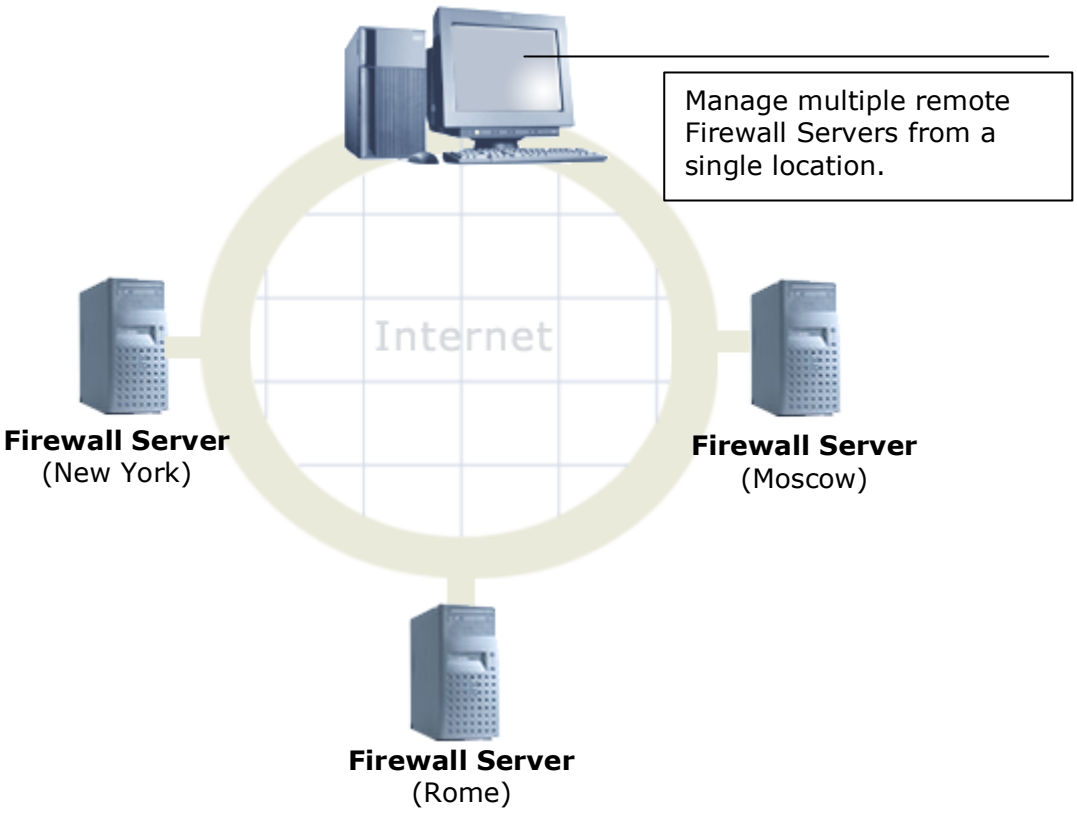
For each rule in the monitor, you will see a name, a description, and the number of packets which have matched the rule.



**Firewall Plugin Log Monitor**
The Firewall Plugin Log monitor displays messages from the firewall security plugin, such as configuration errors. The firewall plugin is the Firewall Server component that provides the advanced rules-based packet filtering and logging.


## 5.6. Remote Firewall Administration

One of the most powerful features of the InJoy Firewall™ GUI is its ability to connect to and manage remote Firewall Servers. This allows network administrators to manage several firewalls from a single physical location.

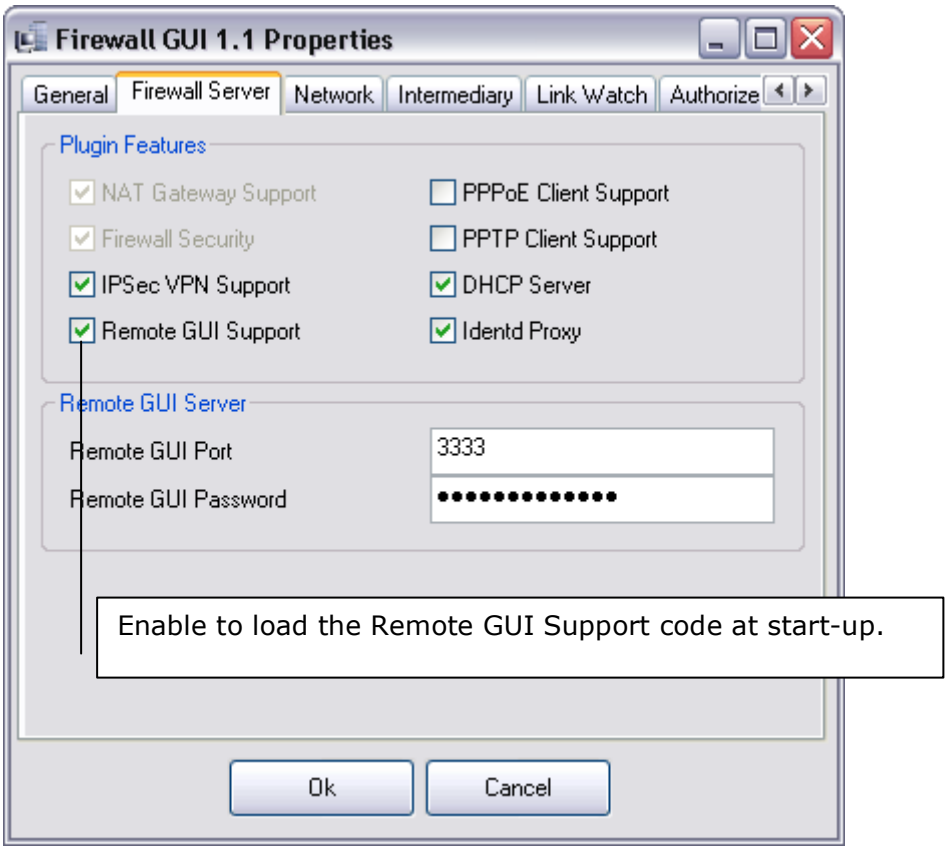



Because the InJoy Firewall™ is a multi-platform product, remote administration capability also allows Firewall Servers on disparate platforms to be managed from the administrator's own preferred desktop platform.

## Configuring the Firewall Server for Remote Administration

Before the Firewall GUI can connect to an InJoy Firewall™ Server, the Firewall Server must be configured to allow remote connections. To enable remote connections for GUI administration, follow these steps:

1. In the Firewall Properties dialog, click on the **Firewall Server** tab and check the **Remote GUI Support** box to enable connections from remote instances of the InJoy Firewall™ GUI.
2. Enter a password in the **Remote GUI Password** box. This password will need to be supplied to the GUI client each time a remote GUI connection is attempted.
3. Inspect the default remote GUI port number shown in the **Remote GUI Port** box. If desired, change this number to suit your needs; this is the port on which GUI connections will be made to this Firewall Server.
4. Click on the **Ok** button to save your settings.




Using the GUI to specify and save the password will ensure that the password is stored encrypted in the file **config\gateway.cnf**.

Remote GUI administration can also be enabled by editing the **config\gateway.cnf** file from your InJoy Firewall™ base install directory. In the file, add the following two lines if they are not already present:

```
GUI-Server = Enabled,
GUI-Password = "mypassword",
GUI-Port = nnnn,
```

You should replace "mypassword" with the password you wish to use for remote administration access and nnnn with the number of the port you wish to use. The default port number for the Firewall GUI is 3333 and will be used

if the GUI-Port variable is omitted. The password should be entered as clear text.

After completing these steps, be sure to restart your InJoy Firewall™ Server to activate your changes.

## Connecting to a Remote Server

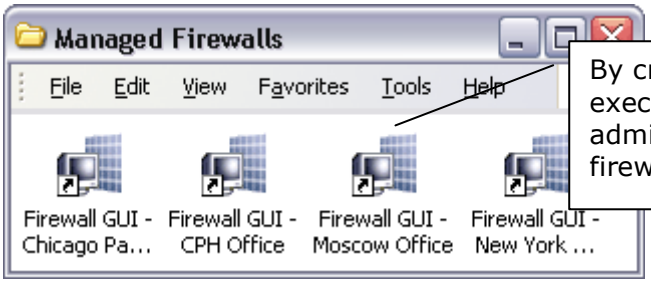
To open the InJoy Firewall™ GUI and connect to a remote Firewall Server from your desktop environment, follow these steps:


1. Open the desktop folder and launch the **Admin Remote Firewall** application in the **Extras** folder.
2. When the Hostname dialog appears, enter the host name or IP address of the remote host into the box and click **Ok**.
3. When the Password dialog appears, enter the password of the remote host's Firewall Server into the box and click **Ok**.

After you have entered the name or IP address of the remote host and the password of its Firewall Server, the Firewall GUI will attempt to open a connection to the remote Firewall Server. If the connection is established successfully, the InJoy Firewall™ GUI will start and you will be able to use it to manage the remote Firewall Server.

## Connecting to a Server at the Command Prompt

At times it is helpful to be able to start remote firewall administration from the command prompt. This is the case, for example, when you wish to create application icons in your desktop folder to automatically connect the Firewall GUI to specific remote Firewall Servers.




By creating desktop folder shortcuts to execute pre-defined GUI connections, administration of multiple remote firewalls can be streamlined.

To start the Firewall GUI for remote Firewall Server administration from the command prompt, supply the remote host name or IP address, port number (optional), and password on the command line as arguments. For example, the following command would attempt to connect the Firewall GUI to a host called *fxserv* on TCP port *2514* with the password *p455word*:


When you enter the fgui command, the Firewall GUI will attempt to open a connection to the remote Firewall Server. If the connection is established successfully, the InJoy Firewall™ GUI will start and you will be able to use it to manage the remote Firewall Server.

You can combine the remote administration and appearance profile features of the Firewall GUI. For example, the following command would connect to *fxserv* once again, but this time on the default port of *3333* using an alternate appearance profile called *remotefw.ini*:


Note that you can use the **-remote** option to launch the Firewall GUI from the command prompt, yet still prompt the user with dialog boxes for a host name or IP address and password.

# 6 The Firewall Deskbar

The InJoy Firewall **Deskbar application** is a HOT new user interface component that can be used to casually monitor and manage Firewall Servers.

With its minimal footprint, the Firewall Deskbar helps to increase available desktop space, while still allowing essential monitoring of the Firewall activity.

To enable the InJoy Firewall Deskbar application, follow the steps discussed in Section 3.4, "Starting the InJoy Firewall™ Deskbar Application."

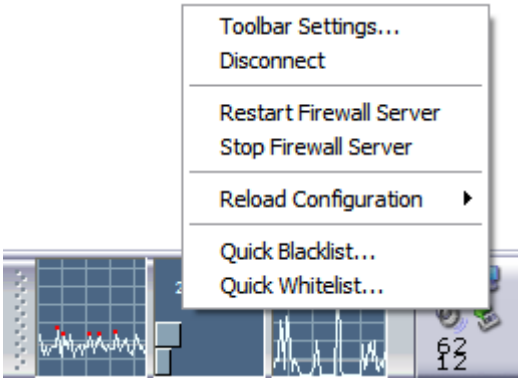
## 6.1. Introducing the Firewall Deskbar

The Firewall Deskbar runs on the **Microsoft Windows** platform, as an Explorer Toolbar application - this means the Firewall Deskbar is basically a client of your desktop, rather than a stand-alone application.

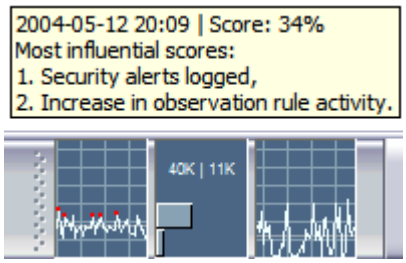
The Firewall Deskbar sits in the Windows taskbar and allows easy monitoring of the intrusion level, network activity, and a wealth of other information.


The main Firewall Deskbar features include:

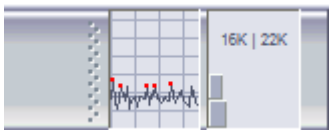
- **Monitoring of local and remote Firewall Servers**
  While the Firewall Deskbar runs ONLY on the Windows platform, it can connect remotely to Firewall Servers running on any of the supported OS platforms. This means you can sit at home, at the Windows PC, and monitor for example a Linux-based Firewall Server thousands of miles away - in real-time on your Windows taskbar. Amazing!
- **A menu with Firewall commands**
  Clicking on the Firewall Deskbar with the right mouse button brings up a pop-up menu, filled with convenient firewall commands and an option to configure the Deskbar.



- **Rapid starting of the Firewall GUI, when clicked**
  Clicking the Firewall Deskbar with the left mouse button immediately starts the Firewall GUI and connects it to the same Firewall Server as the Deskbar is connected to. With this easy option of starting the Firewall GUI, it has become convenient to operate a Firewall Server and you are thus significantly more likely to detect anomalies in time.
- **Tooltip monitors with crucial information**
  When the mouse pointer is placed on top of the various elements of the Deskbar application, contexual tooltips will appear with additional information. These tooltips help you keep track of Firewall Server statistics and other operational information.




- **Highly Customizable**
  On most systems, the Windows taskbar doesn't have much free space to spare; that's why the Firewall Deskbar has been designed so you can resize it freely and also define exactly which monitors to show.




- **Installed seamlessly with the InJoy Firewall**
  The Firewall Deskbar application installs as a Dynamic Link Library (.DLL) to the Windows Explorer process, and can only be enabled from the Windows taskbar. Don't look for an executable to run or an icon to click.

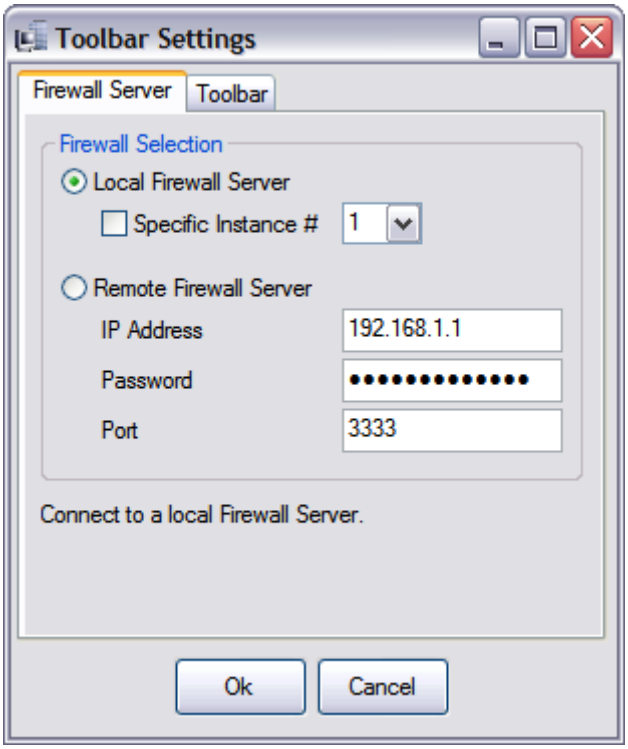
## 6.2. Firewall Deskbar Configuration

To configure the Firewall Deskbar you need to right click its surface and select the "Toolbar Settings…" from the pop-up menu.

### Selecting a Firewall Server

For the Firewall Deskbar to show meaningful information, it must be connected to a **live** Firewall Server.

In the below dialog you specify whether the Deskbar is to connect to a **local** or a **remote** Firewall Server.




**Connecting to a Local Firewall Server**
Select "Local Firewall Server" when the Firewall Server you wish to monitor is running on the same PC as the Firewall Deskbar itself.

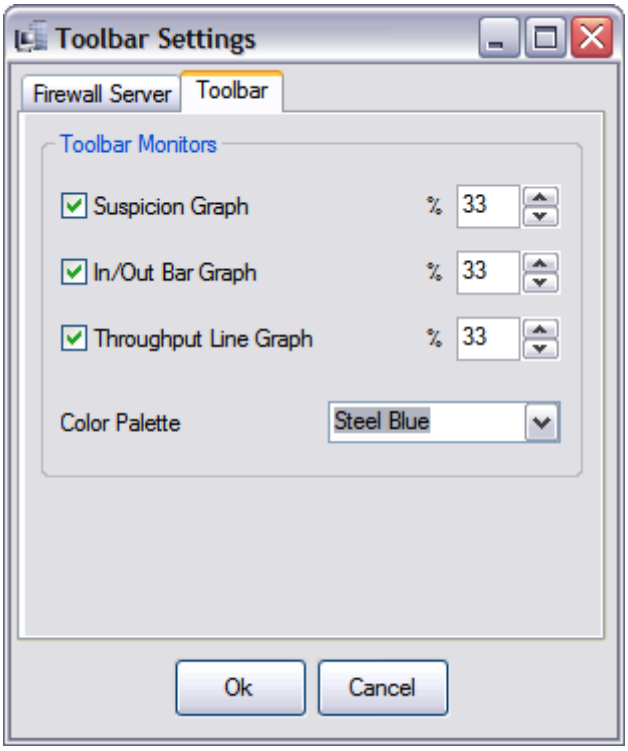
If multiple Firewall Servers run on the same PC, you will need to specify the instance number to monitor. To understand what the instance number is and how to find it, please refer to Section 14.1, "Installing Multiple Firewalls."

**Connecting to a Remote Firewall Server**
Select "Remote Firewall Server" when you wish to monitor a remote Firewall Server over TCP/IP (i.e. over the Internet or your LAN). As with the Firewall GUI, you need to specify the IP address (or a resolvable host name), the remote GUI password of the Firewall Server, and the TCP port to use.

For more information about remote administration of Firewall Servers, please refer to Section 5.6, "Remote Firewall Administration."

### Firewall Deskbar Appearance

On page two of the Toolbar Settings you can control the appearance of the Firewall Deskbar.




The three check-boxes allow you to select which monitor windows that are to make up the Deskbar. To the right of each check-box, you can specify the size of each monitor (as a percentage).

## 6.3. Using the Firewall Deskbar

In summary, the Firewall Deskbar offers these powerful features:

- **A security monitor**, analogue to the suspicion monitor window in the Firewall GUI.
- **Network activity monitors**, analogue to the in/out bar graph and the line graph of the Firewall GUI.
- **Several tool-tip pop-up windows** with statistical information
- **A menu of actions** to easily control the Firewall Server and enforce security.

Below, you can find more information of how to make meaningful use of these features.

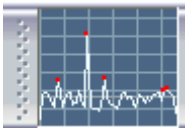
### Using the Suspicion Monitor

The suspicion monitor maintains a visual representation of the attack history, allowing you to weigh any potentially malicious activity against a baseline of questionable traffic.

When a (red) peak raises high above the baseline of suspicion, you can choose to either let the Firewall deal with it, or you can open the Firewall GUI to research security alerts and logs, in detail.

By casually monitoring the suspicion monitor on a daily basis, you develop a habitual sense of the acceptable activity, enabling you to detect and manage any threatening situation, in time.

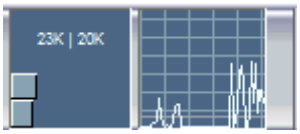
The below screenshot shows the Suspicion Monitor at work, as it looks in the Firewall Deskbar. Notice the single red peak that stands out:



To see how you can easily obtain information about the cause of the red peak, see the section "Understanding the Tool-tips" below.

## Using the Traffic Monitors

The two traffic monitors help you keep an eye on the bandwidth consumption and also discover anomalies in time:



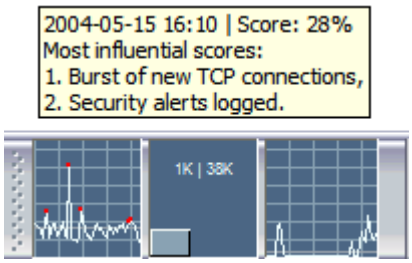

To the left, two bar graphs show the incoming and outgoing traffic. The number of Kilobytes per second is displayed above, with the incoming data rate to the left and outgoing to the right.

For more information about the Deskbar monitor, including the suspicion monitor, please refer to Section 5.4, "Basic Statistics and Information Monitors."

## Understanding the Tool-tips

The Firewall Deskbar offers 3 types of tooltips:

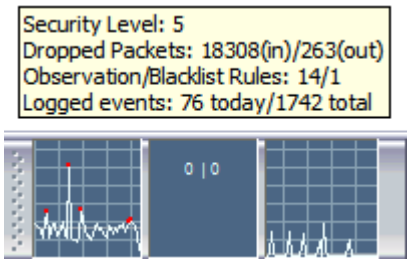
- **Suspicion "red peak" information**
  You get the suspicion tooltip when you point the mouse cursor precisely at the red peak inside the suspicion monitor. Below, the mouse was placed on top of a red peak, and in return, the tooltip explains that the peak was caused by a 28% intrusion/suspicion score.




The most influential reasons for the score was a burst in new TCP connections and security alerts that were logged. If the firewall administrator believes there is reason to study the event in more detail, then that is easy. The administrator should simply make a note of the

time stamp, left click the Deskbar to start the Firewall GUI, and then look at the connection log and the security alert log to see exactly what happened at the time.

- **Security statistics**
  Placing the mouse pointer on top of the suspicion monitor, avoiding the peeks, you will see the below tooltip pop-up:

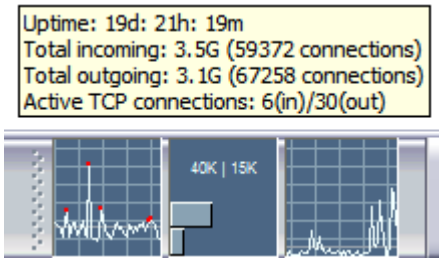



  The tooltip information shows that the Firewall Server is running at Security Level 5. In addition, the tooltip shows statistics about the number of dropped packets, logged events, and the number of active (dynamic) rules.

  The dropped packet count and the logged events are accumulated over time, while the count of dynamic observation/blacklist rules is a real-time representation of the current situation.

  You can use the number of observation rules as an indication of how many situations the Firewall is currently evaluating. For more information about the specific observation and blacklist rules, refer to the standard Firewall GUI monitors.

- **Bandwidth and General statistics**
  Placing the mouse pointer on top of any Deskbar bandwidth monitor, causes the following tooltip to be shown:




  This tooltip shows the uptime of the Firewall Server -- 19 days in this example -- however don't be surprised if you see it being several years :). The total amount of IP traffic and TCP connections that passed through the Firewall is also displayed. At the bottom of the tooltip, you see the current number of active TCP connections.

## Using the Deskbar Pop-Up menu

The Firewall Deskbar pop-up menu displays a meaningful subset of the Firewall actions known from the Firewall GUI. For more information, refer to the Firewall GUI chapter.

## 6.4. Firewall Deskbar FAQ

### Can I manually install and uninstall the Firewall Deskbar

Yes, follow the instructions below to manually install or uninstall the Firewall Deskbar:

**Installation:**

- Place the FXDESKBAR.DLL in the InJoy Firewall folder.
- In a command prompt type:

```
regsvr32.exe /s /c <path>\FXDeskBar.dll
```

- Right click on the Windows taskbar and select the InJoy Firewall Deskbar.

**Uninstallation**

- In a command prompt, type:

```
regsvr32.exe /s /u <path>\FXDeskBar.dll
```

### Where is the Deskbar configuration stored

All settings of the Firewall Deskbar are saved in a single plain-text INI file.

The location of the INI file is:

- `%Windows%\fxtoolbar.ini`

### Can I drag the Firewall Deskbar to the desktop

Yes, however it has been tested only for proper operation within the Windows taskbar. Dragging it to Desktop area will generally work, with some exceptions in terms of resizing. Use trial and error.

### Can I have multiple Firewall Deskbars installed?

No, not possible.

### Is the password saved in encrypted form?

Yes!

### Need I stop the Deskbar to install a new InJoy Firewall

No, a new InJoy Firewall installation can automatically replace the Firewall Deskbar, even when they are in use. You will however need to reboot for Windows to load the updated files.

# Part III
# Working with the InJoy Firewall™

# 7 More about Configuration

Before making more advanced changes to the InJoy Firewall™ Server configuration or the security policy, you should take a moment to study the information in this section. The following subjects are discussed:

- The nature and benefits of the InJoy Firewall™'s modular plugin architecture and how it impacts the configuration process.
- InJoy Firewall™ configuration basics, including an overview of the configuration options, the possible configuration methods and their benefits.
- The format of the Firewall Server configuration file, how to make configuration changes in plain text and where to find out more.
- How to activate configuration changes.

This section provides insight into the structure of the InJoy Firewall™ Product and it should be considered essential reading if you are installing the InJoy Firewall™ for the first time.

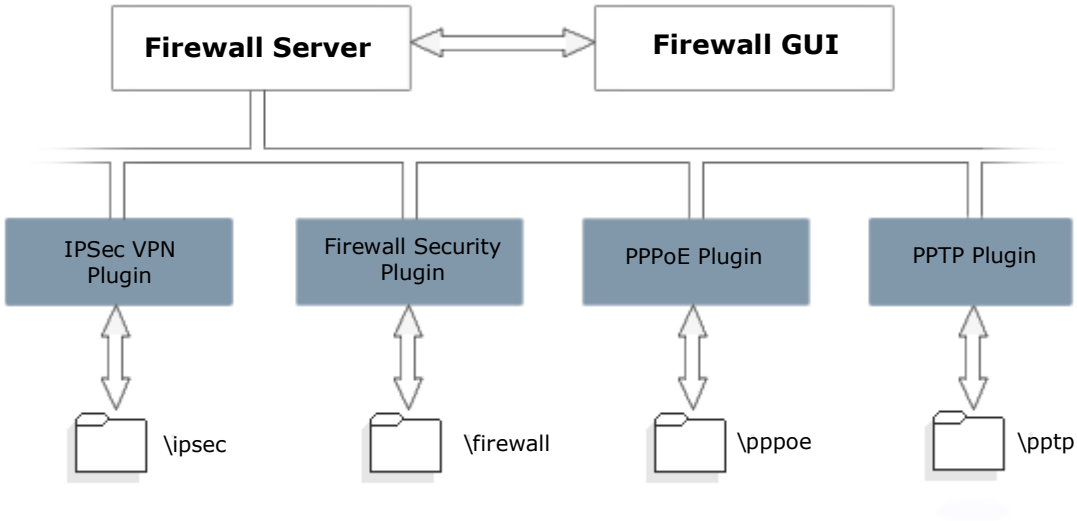
## 7.1. Plugin Architecture

Because configuration requirements are different, many of the InJoy Firewall™ plugins are also accompanied by their own plugin-specific documentation and configuration options.

By covering functionality-specific topics in plugin-specific guides, you don't need to wade through documentation and options for features that you won't use anyway. Instead, just the information you want is presented quickly and concisely in focused configuration files and configuration guides.

## Understanding the InJoy Firewall™ Plugin Architecture

Much of the functionality offered by the InJoy Firewall™ comes from a series of feature plugins.




The feature plugins each store their configuration information in separate, plugin-specific configuration file(s). This simplifies the task of making needed configuration changes to a particular Firewall function. For example, the PPPoE Plugin uses the PPPoE sub-directory and the configuration file pppoe.cnf. For a complete roadmap of the InJoy Firewall™ configuration files, please refer to Appendix 11.

Most of the Plugin features can be configured through the InJoy Firewall GUI and they can always be edited directly in the plain text configuration files.

# 7.2. InJoy Firewall™ Configuration

As seen in section 4, it is generally a very intuitive and straight-forward procedure to configure the InJoy Firewall™. However, it helps to have a better understanding of the underlying design and configuration methods when it comes to configuring some of the more complex plugin features.

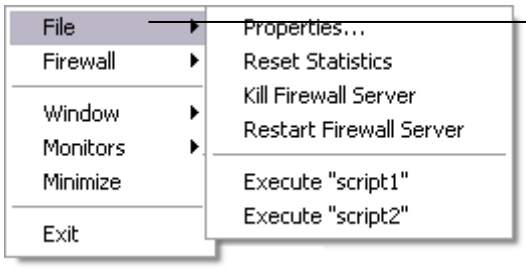
## Firewall Server and Plugin Configuration

The InJoy Firewall™ Server offers two groups of configuration options:

- **General Firewall Properties**

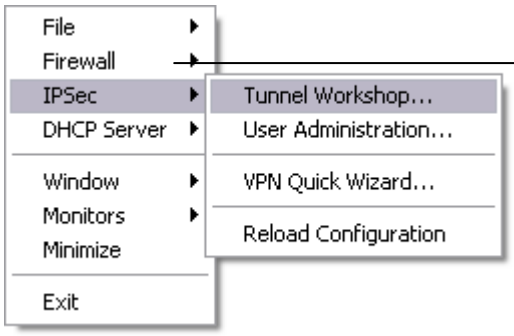
The Firewall Properties offer a set of global options that define the general behavior of the InJoy Firewall™ product. This includes the product registration key, the selection of active plugin features and the internal network definition.

The Firewall Properties are configurable through the InJoy Firewall™ GUI or by editing them in the file **config\gateway.cnf**.




The basic InJoy Firewall™ GUI pop-up menu, when only the Firewall Security plugin is loaded.

- **Plugin Specific Features**
  The InJoy Firewall™ supports a modular plugin configuration structure that is consistent with its modular architecture. For example, if you wish to set up an IPSec based VPN you would enable the IPSec Plugin. When the Firewall is restarted the GUI will hold an extra menu-item in the pop-up menu, allowing you to configure the IPSec functionality.




Plugin Features, such as the Firewall Security Plugin, IPSec and the DHCP Server Plugin, provide their own add-in configuration support to the Firewall GUI.

## Available Configuration Methods

To configure the InJoy Firewall™ you can choose among two methods.

**GUI Configuration**
This is an ideal option for first time configuration and for beginners. The option supports On-screen help and input validation features that help prevent misconfiguration.

**Plain-text Configuration**
While GUI configuration is possible for most of the critical features, you will find that there are usually some extra expert-level options available in the plain text configuration files.

Note that configuration using a word processor rather than a text editor requires that the administrator take care to save and load files in "plain text" format.

## 7.3. Plain-text Configuration

### The Firewall Server Configuration File

The main configuration file used by the InJoy Firewall™ Server is stored in the InJoy base install directory, in the file **config\gateway.cnf**. As is the case with most InJoy component configuration files, the file can be edited using a basic text editor, such as Notepad for Windows.

In the main configuration file, you'll find a number of options, one per line, which control various aspects of the Firewall Server's operation. Most of these options have a close match in the Firewall Properties dialog of the InJoy Firewall™ GUI. Here is a segment from the **config\gateway.cnf** file:

```
Internal-Net-3 = ”172.16.0.0”,
Internal-Netmask-3 = ”255.31.0.0”,
PPPoE = Disabled,
PPTP = Disabled,
IPSec = Enabled,
DHCPd = Disabled,
Fragment = Enabled,
MTU = 1500,
MSS-Adjust = 1200,
```

To edit InJoy components' plain-text configuration files, follow these guidelines:

- Options with **Enabled** or **Disabled** as their value can be thought of as toggles. Edit the line to read 'Enabled' if you would like a feature or plugin to be activated, or 'Disabled' if you would like it to be deactivated.
- Options with other values are similar in function to GUI text entry boxes. Replace the existing value with a new one, taking care to preserve quotation marks, if present.
- To see the complete list of configuration attributes and their default values, consult the file **template\gateway.cnf**.

Full details on the options which can appear in **config\gateway.cnf** and descriptions of the individual parameters can be found in Appendix 12.

### Plugin Configuration Files

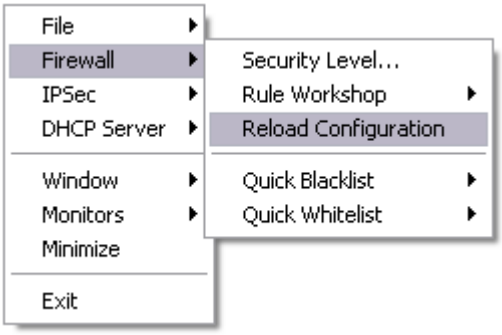
Making configuration changes to the feature plugins is essentially the same as making configuration changes to the Firewall Server configuration file.

For a quick overview of all the available configuration files in the InJoy Firewall™, please refer to Appendix 11.

## 7.4. Activating Configuration Changes

There are two options for activating configuration changes that are made through a text editor or through the Firewall GUI.

- Use the Firewall GUI to cause the configuration file in question to be re-read. Several of the submenus in the Firewall GUI, including **Firewall**, **IPSec** and **DHCP** include the "Reload Configuration" option.




- Use the **sync** command in the base install directory of the InJoy Firewall™ to cause the configuration file in question to be re-read. Use the **-firewall**, -**ipsec**, and -**dhcp** options to cause the Firewall Server, IPSec VPN Plugin or DHCP Plugin configuration files to be re-read.


When you have successfully reloaded your firewall's configuration, you will see confirmation messages on the firewall console and in the firewall activity log:

```
Firewall: Refreshing configuration
Firewall: Configuration refreshed!
```

Once you have received the confirmation message, any changes you have made to your firewall's configuration are active.

After manually editing configuration files for which there is no re-read option, such as the "Firewall Properties", you need to re-start the Firewall Server in order to have your changes take effect.

**Note:** When activating a new configuration, the plugin will need to virtually restart itself. This causes current run-time information – such as the list of TCP connections and VPN tunnels – to be cleared.

# 8 Using the InJoy Firewall™

A number of different tasks comprise the day-to-day operation of the InJoy Firewall™. Among these tasks are:

- Observing the InJoy Firewall™ as it operates to ensure that network traffic is being handled as expected.
- Setting and managing security preferences for the Firewall Server to ensure that functionality is preserved while threats are minimized.
- Maintaining a balance between firewall functionality and firewall performance by tuning your preferences accordingly.
- Tracing packets as necessary to observe problem activity.

These tasks and others related to everyday operation of the InJoy Firewall™ in a deployed environment will be discussed in this section.

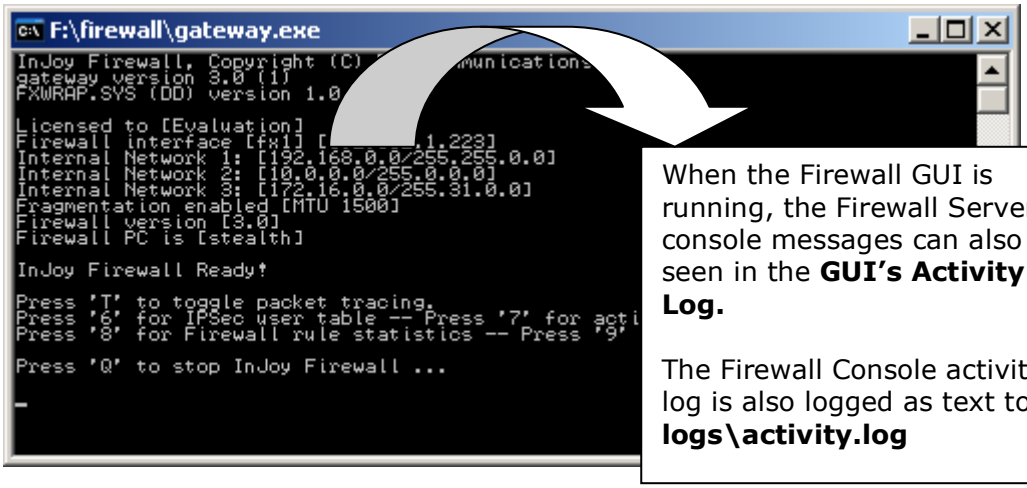
## 8.1. Verifying Basic Firewall Operation

There are several ways to monitor firewall activity and the traffic that flows through it. Taking advantage of these features will ensure prompt detection of any anomalous activity.

### Firewall Server Console and Activity Log

The Firewall Server Console and Activity Log provide general messages and information on key operational aspects of the InJoy Firewall. This includes critical messages about Firewall Server activity such as malfunction, starts and stops, messages about Firewall GUI connections, and messages from the firewall plugins.

The Firewall Server console and Activity Log monitor provide an important forum for the monitoring of firewall stability and operations.




When the Firewall GUI is running, the Firewall Server console messages can also be seen in the **GUI's Activity Log.**

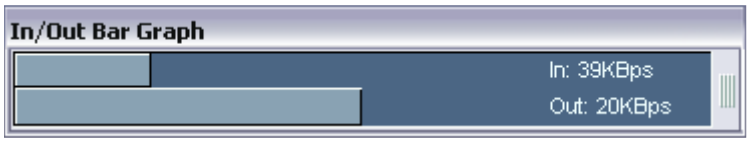
The Firewall Console activity log is also logged as text to **logs\activity.log**

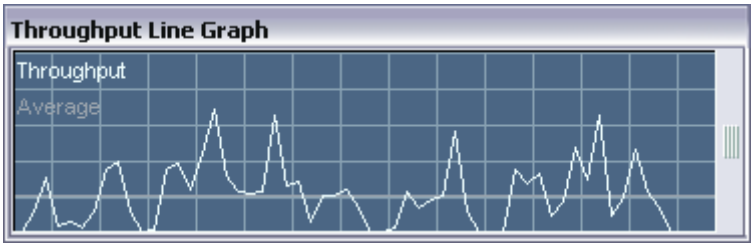
## Traffic Indicators

Following installation, it is important to ensure that the InJoy Firewall™ scans traffic as expected. For instance, if the InJoy Firewall™ is installed to the wrong network adapter, you would see it as operational, but you would not be protected against threats from the Internet.

Another typical source of invalid Firewall behavior stems from wrong configuration of the internal networks. If the internal networks (found in the **"File | Properties"** settings) are incorrectly configured, the InJoy Firewall™ might be tricked into seeing incoming traffic as outgoing and vice versa.

To quickly determine whether traffic is handled correctly, the InJoy Firewall™ GUI includes different traffic monitors. These traffic monitors allow you to quickly verify the amount of data being scanned and also that the Firewall is able to correctly determine the traffic direction. The traffic monitors include the Throughput Bar Graph, the In/Out Bar Graph, the Throughput Line Graph and the Info Monitor.


In the above figures, the Firewall user was downloading a file and from looking at the monitors, it can be determined that the incoming traffic stream is constant at 40Kbytes per second. This suggests that both the traffic

direction and the full amount of data are correctly being scanned by the Firewall.

### Using Other Monitors

Several other monitors are available for determining the operational state of the Firewall. The Firewall GUI includes monitors that provide details about loaded plugins, active connections, connections which have occurred in the past, IP addresses which have been blacklisted, or rules which are currently active and how many times each rule has been matched by traffic.

For more information on the purpose and role of any particular monitor, please refer to Section 5.4, "Basic Statistics and Information Monitors." and section 5.5, "Advanced Firewall GUI Monitors."

## 8.2. Checking Firewall Logs

Firewall logs provide the network administrator with a record of *(questionable)* activity over time. This information can be used to verify the security policy, correct configuration problems, construct new firewall rules, carry out investigations, and perform other useful security tasks.

The InJoy Firewall™ keeps its logs in plain text format, allowing them to be opened or searched using any tool which operates on plain text files.

### Viewing Log Files

All InJoy Firewall™ logs can be viewed in the following ways:

- Using the Firewall GUI with its predefined monitors.
- Manually with a plain text editor.
- In the customizable Logview tool (section 10.4).

### Types of Log Files

Two types of log files are maintained by the InJoy Firewall™:

- Firewall System Logs
- Firewall Security Logs

### Firewall System Log Files

All the InJoy Firewall™ features and plugins occasionally need to output basic configuration and run-time alerts. The InJoy Firewall™ keeps its System Logs in the base InJoy installation path, in the **logs** sub-directory.

The following System Logs are maintained by the InJoy Firewall™:

- **activity.log** contains the Firewall Server's activity log—the same information displayed on the Firewall Server console and in the Firewall Server Console monitor of the Firewall GUI.

  This file is deleted each time the InJoy Firewall™ Server is restarted and usually doesn't grow beyond a few Kbytes in size.

- **firewall.log** contains log entries made by the firewall plugin, such as configuration problems, configuration reloading and supported Firewall Features. This file does **not** contain security related information.

The maximum size of this file is 5MBytes and automatic deletion of the file takes place when the limit is reached.

- **dhcpd.log** contains log entries related to the activity of the InJoy Firewall™ Dynamic Host Configuration Protocol (DHCP) plugin.

  This file grows indefinitely, with no limits and no automatic deletion.

- **ipsec.log, vpn-auth.log and Pluto.log** contain log entries related to Virtual Private Networking (VPN) using the IPSec plugin.

  The maximum size of these files is 10MBytes and automatic deletion of the files take place when the limit is reached. The 10Mbytes limit is configurable in ipsec/options.cnf.

- **pppoe.trc** contains activity messages from the PPP over Ethernet (PPPoE) plugin.

  This file grows indefinitely, with no limits and no automatic deletion.

- **pptp.trc** contains activity messages from the Point to Point Tunneling Protocol (PPTP) plugin.

  This file grows indefinitely, with no limits and no automatic deletion.

- **status.gw** contains runtime information about the Firewall Server process(es) currently running on the system, including the physical interface to which each server is bound.

  This file has a static size and it is overwritten with each Firewall restart.

### Firewall Security Log Files

Security Logs are exclusively generated by the Firewall Security Feature Plugin. The logging of security events occur to the **firewall\logs** subdirectory in the InJoy Firewall™ base directory.

**For a roadmap of the plain text logs created by the Firewall Security Plugin, please refer to the "Firewall Security Guide".**

## 8.3. Managing Firewall Security

Because no two networks or computer systems are alike, the InJoy Firewall™ provides powerful, flexible features to manage the security configuration of the Firewall Server. Not everyone is a network security expert; The InJoy Firewall™ therefore makes these features accessible, easy-to-use and provides a well-conceived set of default behaviors.

### Default Security Level

The default configuration of the InJoy Firewall™ provides a good starting point for securing most users' small to medium-sized networks.

By default, the InJoy Firewall™ provides firewall protection for one external network interface, as well as traffic forwarding (NAT Gateway capability) between this external interface and the internal interfaces.

The default security configuration of the InJoy Firewall™ represents an initial security level of 5, as set using the Firewall GUI's Security Level dialog.

The security level 5 setting represents a good balance between security, functionality and network performance. It can, however, be easily changed if necessary.

**Default Security Policies**
The default security policy of the InJoy Firewall™ is to:

- Deny all ICMP packets except those of types 0, 3, 8, or 11. These ICMP types are needed in order for Ping and Traceroute to function.
- Allow outgoing NAT connections
- Block all firewall ports
- Leave e-mail unfiltered and unmodified

This default security policy creates a generally secure environment for most networks without administrators having to worry about losing network functionality.

**Default Firewall Rules**
In addition to the default security policy, a number of packet filtering and firewall rules are also enabled in the default InJoy Firewall™ configuration. These include:

- Basic notification of all logging and blacklisting activity
- Logging of all ping, trace-route, port scans and other suspicious ICMP packets to the Security Alerts monitor
- Logging of all connections to popular TCP ports to the Security Alerts monitor.
- Logging of all inbound and outbound TCP connections to the Connection Log monitor.
- Logging of all rejected packets to the Dropped Packets monitor.
- Logging of all rejected TCP connections to the Rejected Connections monitor.
- A warning once 30 packets from a specific host have been dropped
- Rejection of incoming URL requests bigger than 1024 bytes
- Rejection of packets bigger than 6144 bytes
- Denial of file or printer sharing requests using any protocol family

This ruleset logs generally suspicious network events and blocks a number of potentially dangerous ones. Together with the default security policy, it provides a solid platform for your network's basic security.

## Selecting a different Security Level

You can choose to operate your Firewall at one of a number of pre-defined security levels using the InJoy Firewall™ GUI's Security Level dialog. To open the Security Level dialog, select **Firewall**, then **Security Level**, in the Firewall GUI pop-up menu. This will cause the Security Level dialog to open.


The Security Level slider in the Security Level dialog allows the firewall administrator to choose from eleven security level presets, ranging from level zero (least strict, less security) to level ten (most strict, more security). Notice that as you move the slider up and down, a concise description of the security policy implemented by the chosen level is shown in the box to the right of the slider.

The collection of security policies implemented by the security level can be arranged into n major groups, each successively stricter than the last:

- **Security levels 0-3 (least secure)** allow all ICMP packet types. Outbound NAT traffic is allowed. Firewall ports are open and Safe-Mail (for handling suspicious e-mail attachments) is disabled.
- **Security level 4** allows a limited selection of ICMP packet types. Outbound NAT traffic is allowed. Firewall ports are open and Safe-Mail is disabled.
- **Security level 5** allows a limited selection of ICMP packet types. Outbound NAT traffic is allowed. Firewall ports are blocked and Safe-Mail is disabled.
- **Security levels 6-7** allow a limited selection of ICMP packet types. Outbound NAT traffic is allowed. Firewall ports are blocked and Safe-Mail is configured to automatically rename incoming e-mail attachments that might pose a risk.
- **Security level 8** allows a limited selection of ICMP packet types. Outbound NAT traffic is allowed. Firewall ports are blocked and Safe-Mail

is configured to automatically discard incoming e-mail attachments that might pose a risk.

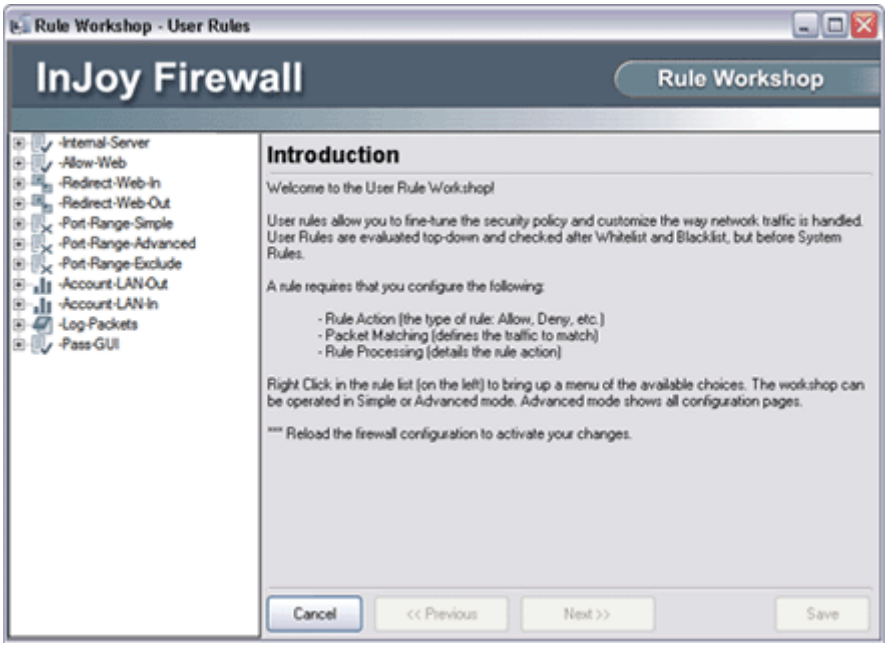
- **Security level 9 (most secure)** all traffic is rejected by default. Firewall ports are blocked and Safe-Mail is configured to automatically discard any incoming e-mail attachments.
- **Security level 10 (VPN)** allows only secured IPSec VPN traffic and DNS lookups by default. Firewall ports are blocked and Safe-Mail is disabled.

Even though the general policy for some security levels is the same, you should take care to read the description of the security level carefully; the list of active rules grows progressively stricter as security levels increase.

## The Rule Workshop

The InJoy Firewall™ includes a powerful rule system that allows administrators to filter traffic in several ways and according to very specific guidelines. The Firewall GUI features an easy-to-use, yet powerful rules editor called the Rule Workshop to help administrators manage firewall rules.

To start the Rule Workshop, select "**Firewall | Rule Workshop | User Rules"** in the Firewall GUI pop-up menu. This will cause the Rule Workshop to appear.




On the left side of the Rule Workshop, you will see a panel showing a tree of all existing rules. To view a rule, click on it and its details will be shown on the left side of the Rule Workshop, where you can change them easily.

To create a new rule, right-click in an empty area of the left panel and select **Create Rule**. A wizard will guide you through the process of creating your new rule.

After creating rules, you can move the currently selected rule up or down in order of precedence by clicking on the **Up** and **Down** buttons on the right side of the Rule Workshop dialog. As you click to move a rule is moved up or down, you will see its position in the rules tree on the left side of the dialog move up or down accordingly.

Additional, more detailed information on the Rule Workshop, on the editing of plain text rule configuration files directly, and the functions of various rules can be found in the ”InJoy Security Guide.”

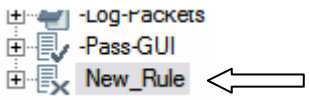
## Blocking and Unblocking Ports

Depending on the security level or other options in the Security Level dialog you have chosen, the ports on your firewall’s external interface may be either blocked or unblocked.

After setting your basic security level accordingly, you will therefore usually need to create exceptions to this policy to either block or unblock specific ports on the firewall, depending on the selection of other services that your Firewall does or doesn’t provide. This is done using the Rule Workshop (refer to the previous section for details on starting the Rule Workshop).

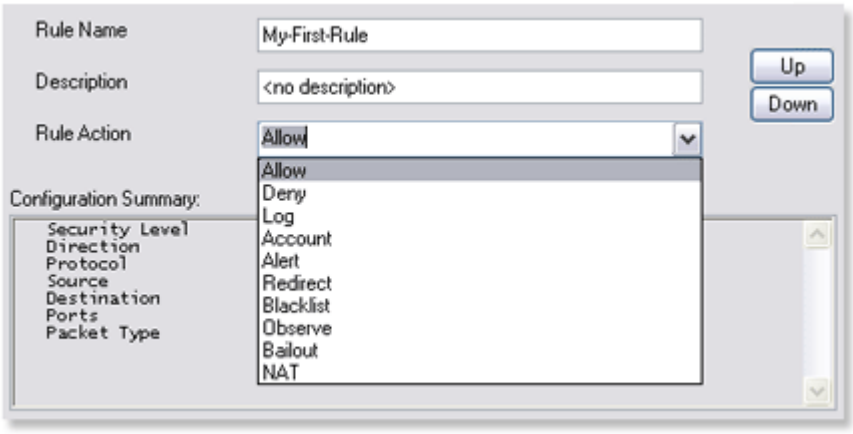
To unblock an otherwise blocked port, follow these steps:

1 Right-click in an empty area of the rules tree (left side of Rule Workshop window) and select **Create Rule** to create a new rule. A new rule will appear, selected, at the bottom of the tree.




2 Enter a name for the new rule in the **Rule Name** box and a description in the **Description** box.

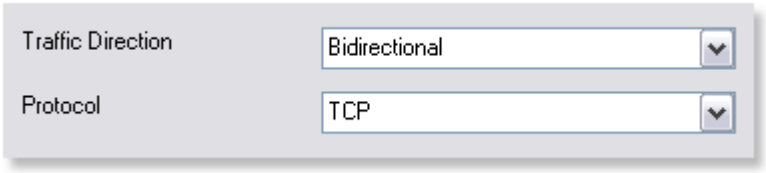
3 In the **Rule Action** drop-down box, choose **Allow**.




4 Click on the **Next** button to display the Packet Matching options.

5 In the **Packet Direction** drop-down box, choose one of the four options, depending on whether you want to filter **Incoming** traffic, **Outgoing**, **Bidirectional** traffic, or simply **Ignore** the direction of the packet.

6 In the **Protocol** box, select the transport layer protocol you want to filter, or **Ignore** to apply this rule to any packet type.

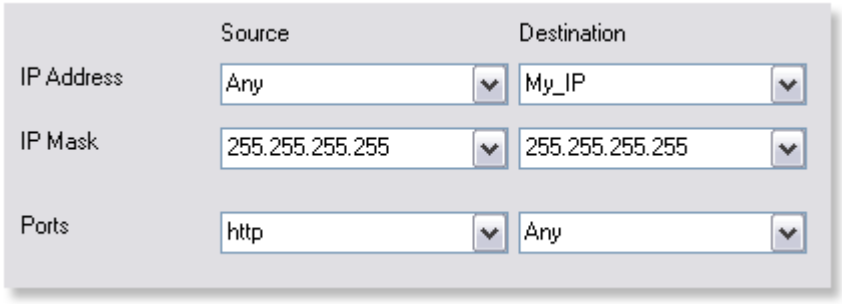



7 Click on the **Next** button to display the TCP/IP options.

8 Select either **Any**, **My_IP**, or enter an IP address into the Source and Destination **IP Address** boxes to match any IP address, the IP address of the firewall, or a particular IP address, respectively.

9 Select or enter a netmask for matching in the Source and Destination IP addresses in the two **IP Mask** boxes.

10 Select or enter the Source and Destination ports that you want to match in the **Ports** boxes.




11 Click Save to save the new rule.

12 Move the rule up or down within the rules tree until it is applied in the order desired with respect to other filtering rules.

The process to block an otherwise unblocked port is similar; simply select **Deny** instead of **Allow** from the **Rule Action** drop down box mentioned in step number three (3).

Firewall ports can also be blocked or unblocked manually by editing the **firewall\firerule.cnf** file using a text editor such as Notepad or Emacs. The basic format for a rule to block or unblock traffic from a specific host is:

```
My-Port-Rule-Name
     Source = ”match.ip.addr.here”,
     Source-Netmask = ”match.net.mask.here”,
     Destination-Port = ”port”,
     Rule-action = Allow|Deny
```

For example, to unblock port 3333, the default Firewall GUI port, for requests from the host 204.127.202.8, you could add the following text to **firewall\firerule.cnf**:

```
Allow-Firewall-GUI-Access
     Source = ”204.127.202.8”,
     Source-Netmask = ”255.255.255.255”,
     Destination-Port = ”3333”,
     Rule-action = Allow
```

To block or unblock a port for all hosts, omit the Source and Source-Netmask variables from the rule specification.

For additional discussion of rules, processing options such as rule match logging, and the steps involved in creating other types of rules, please refer to the ”InJoy Security Guide.”

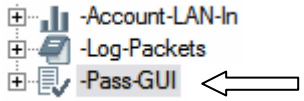
After changing the **firewall\firerule.cnf** file or creating new rules using the Rule Workshop, be sure to reload the Firewall Server configuration to make your changes active.

## Unblocking the Firewall GUI Port

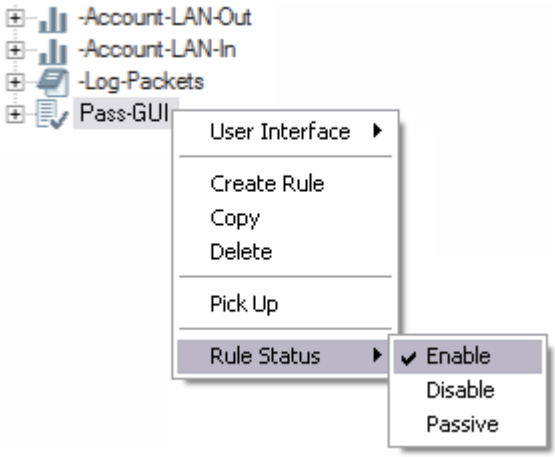
If you plan to use the Firewall GUI **from a remote host** to manage your local Firewall Server, you must unblock the Firewall GUI port on your firewall. To unblock the Firewall GUI port, you can either follow the instructions given in the previous section or simply use the rule workshop to enable the included sample rule. The sample rule assumes the default Firewall GUI administration port is 3333.

To enable the included GUI allow rule, follow these steps:

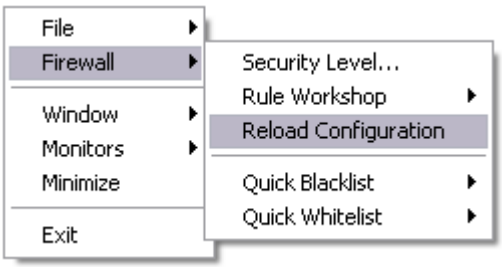
1. Start the Rule Workshop by selecting **Firewall, Rule Workshop** and then **User Rules** in the Firewall GUI pop-up menu. This will cause the Rule Workshop to appear.
2. Locate the “Pass-GUI” Rule:




3. Enable the “Pass-GUI” rule in the rule-list, by right-clicking on its name and selecting **Rule Status**, then **Enable**. When the prefixed **‘-’** sign disappears from the rule name, the rule is no longer disabled.




4. Reload the Firewall configuration to activate your changes.



CAUTION: After having reloaded the Firewall Configuration, traffic to the Firewall Server on port 3333 is accepted from any remote host and only the GUI password check will prevent outsiders from taking control of your Firewall.

The Pass-GUI rule is also easily edited in the plain text rules.

```
Pass-GUI      Rule-Status = Enabled,
              Comment = "Pass Remote GUI traffic (port 3333 by default)",
              Source-Port = "3333",
              Direction = Bidirectional,
              Rule-Action = Allow
```

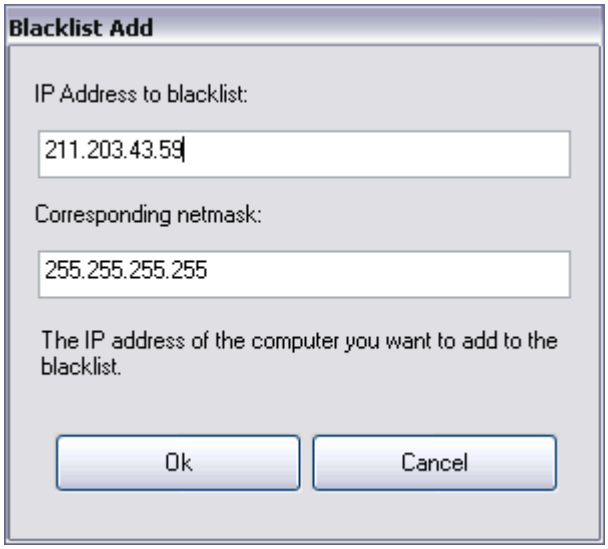
Note: Because the rule is ”Bidirectional” it allows traffic on port 3333 in both directions – both incoming and outgoing.

## Quick Blacklisting and Whitelisting

Blacklisting and whitelisting give the Firewall Administrator an easy way to create a special rule for all traffic related to a specific host. A blacklist will block a host; a whitelist will unconditionally allow traffic from a host that might otherwise be blocked.

To quickly blacklist a host, follow these steps:

1. In the InJoy Firewall™ pop-up menu, select **Firewall**, then **Quick Blacklist**, then **Add**. This will cause the Blacklist Add dialog to appear.
2. In the upper text box, enter the IP address of the host or hosts that you wish to add to the blacklist.
3. In the lower text box, enter the netmask to apply to this IP address for blocking purposes.
4. Click **Ok** to add the host(s) to the blacklist.




To remove a host from the blacklist, reverse the above procedure by entering the same values, but pick “Remove” from the menu instead of “Add”.

To manipulate the whitelist, follow the same steps but use the **Quick Whitelist** menu instead.

For example, to block all traffic from 207.214.14.3, you could add the following text to **firewall\blacklst.cnf**:

```
My-Blacklisted-Host-Feb15
     Source = ”207.214.14.3”,
     Source-Netmask = ”255.255.255.255”,
     Rule-action = Deny
```

Similarly, to unconditionally allow all traffic from 208.196.1.3, you could add the following text to **firewall\whitelst.cnf**:

```
My-Whitelisted-Host-Feb15
     Source = ”208.196.1.3”,
     Rule-action = Allow
```

Note that blacklist or whitelist rules added manually should be removed either manually or via the rule workshop. Trying to remove a manually entered blacklist rule from the “quick blacklist” interface is not recommended.

After you have edited the **firewall\blacklist.cnf** or **firewall\whitelst.cnf** files or added to your blacklist or whitelist using the Firewall GUI, be sure to reload the Firewall Server configuration to make your changes active.

## Using the identd Proxy

Identd is an authentication server protocol used widely to authenticate Internet Relay Chat (IRC) clients and other applications.

Standard NAT-based Internet Gateway capability does **not** provide for the incoming identd requests to pass through the Firewall, so to allow remote servers to authenticate IRC clients on your network, a special ident proxy server must be started on the Firewall PC. The InJoy Firewall includes such a server, capable of acting as a proxy for the other PCs on your private LAN.

When the identd proxy is enabled, the Firewall will attempt to forward identd requests from the Internet to the correct client’s identd server on the internal network, thereby transparently enabling identd service through the Firewall. If the identd proxy is unable to determine which internal PC that is responsible for the incoming request, it will respond autonomously.

It is recommended, however only widely required by IRC servers that you enable the identd proxy server. **The benefits of enabling identd**, is that remote servers of any type can authenticate your identity and safely allow you to login with your IRC, mail or web-browser clients. **The consequences of disabling identd** can be inability to use IRC clients and it can also lead to minute long delays when using mail-clients and other client software.

The identd proxy can be enabled or disabled from within the Firewall Properties dialog. For details on how to do this, please refer to Section 4.3, “Selecting Plugin Features.”

To enable or disable the identd proxy without using the Firewall GUI, load the **config\gateway.cnf** file into a text editor such as Notepad or Emacs and edit the value of the **Identd** variable to either **Enable** or **Disable**. For example, the following line enables the identd proxy and also sets your identity:

```
Identd = Enable,
Identd-User = "Peter",
```

After changing the **config\gateway.cnf** file, you need to restart the InJoy Firewall™ Server to activate the change.

**Note:** by enabling the identd proxy, TCP port 113 will be opened on your Firewall PC. Open ports always provide a potential security risk, as well as offering hackers a way to detect the presence of your PC. If security is your absolute top-priority, then it is recommended that the identd proxy is left disabled.

## Using the Safe Mail Proxy

The Safe Mail proxy is a Simple Mail Transfer Protocol (SMTP) proxy designed to protect users and SMTP servers from various types of malicious or questionable e-mail activity. Among others, the Safe Mail proxy provides the following security-oriented features:

- The ability to filter out or inactivate e-mail attachments which might contain worms or viruses
- The ability to limit contact with your SMTP server to connections from a list of trusted hosts
- The ability to limit the maximum size of incoming e-mail before it reaches your SMTP server
- The ability to filter out malformed or malicious SMTP sessions designed to compromise your SMTP server

The Safe Mail proxy can be enabled from the Security Level dialog. Follow these steps to enable the Safe Mail proxy and configure it:

1. In the Firewall GUI pop-up menu, select **Firewall**, then **Security Level**.
2. Check the **Safe Mail Proxy** box in the Security Level dialog to enable the Safe Mail proxy.
3. Click on the **Custom** button in the Security Level dialog to open the Security Level Configuration dialog.

4 Click on the **Safe Mail** tab to open the configuration panel related to the Safe Mail proxy.


In the Safe Mail configuration area, you will see several configurable options related to operation of the Safe Mail proxy.

In the **Executable Attachments** area, you can specify a list of attachment extensions which are assumed to be questionable and an action which should be performed whenever an attachment with a matching extension passes through the Safe Mail proxy. The default list of extensions is adequate for most users. The list of possible actions includes:

- **Rename** to modify the attachment in question so that its extension become "*.QQQ", thereby preventing accidental execution
- **Deny** to simply remove the attachment in question from the message before forwarding it to the SMTP server
- **Log** to log the receipt of a potentially damaging attachment to the Firewall Security Alert log.

In the **SMTP Control** area, you can provide information about your SMTP server. To configure Safe Mail for your SMTP server, follow these steps:

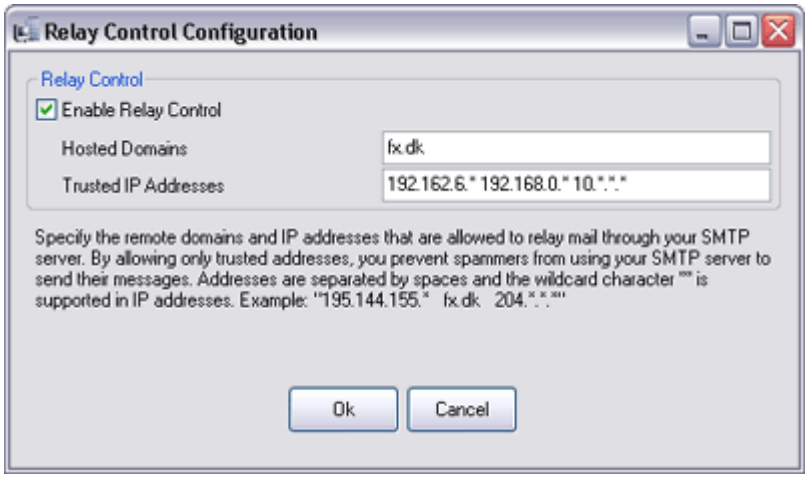
1 In the **Redirect to internal server** box, enter the IP address of your SMTP server or select **My_IP** if your SMTP server runs on the same machine as your firewall.

2 In the **Maximum Email Size** box, enter the size limit for incoming e-mail, in kilobytes, or select **Unlimited** if you do not wish to limit the size of e-mail messages which will be forwarded to your SMTP server.

3 If you wish to enable relay control to prevent unauthorized hosts from using your SMTP server (recommended), click **Configure** to open the

Relay Control Configuration dialog and proceed with steps four, five and six.

4 In the Relay Control Configuration dialog, check the **Enable Relay Control** box to enable relay control.




5 Enter the domains of your networks into the **Hosted Domains** box and the IP address ranges for trusted hosts into the **Trusted IP Addresses** box. These are the machines that will be allowed to use your SMTP server.

6 Click **Ok** to close the Relay Control Configuration dialog and save your changes; then click **Ok** again to close the Security Level Configuration dialog and save your changes.

After making changes to your Safe Mail proxy configuration, be sure to reload the Firewall Server configuration to make your changes active.

## 8.4. Firewall Performance Tuning

Though the InJoy Firewall™ is designed to run efficiently and unobtrusively in the background, some firewall functions consume more system resources than others. It is therefore important that firewall users remain aware of the current firewall configuration.

### Observed Connections

Observed connections are the number of incoming or outgoing connections that will be watched and that will therefore appear in the Firewall GUI monitors.

The default number of observed connections is 2000 and the greater the number of connections being observed, the greater the drain on system resources.

To change the number of observed connections from the Security Level dialog, follow these steps:

1 Click on the **Custom** button at the bottom of the **Security Level** dialog.

2 Click on the **General** tab in the configuration dialog that appears.

3 In the **Max Connections** box, enter the number of connections you want observed.

4 Click **Ok** to save your changes.

Note that connections which occur beyond the limit of simultaneous observed connections will be treated exactly as any other kind of traffic would, given your security level and firewall rules; connections beyond the observed connections limit will simply not appear in monitoring tools.

## Dynamic Rules

Dynamic rules are rules that are created based on real-time activity from hosts on the external network. If a remote host repeatedly attempts to violate the running set of firewall rules, the host will be temporarily added to an IP address observation list or become blacklisted (to prevent all further connection attempts).

The default maximum number of dynamic rules is 1024 and the greater the number of dynamic rules created, the greater the potential drain on system resources.

Limiting the number of possible Dynamic Rules should be done with great care and only when absolutely required, as it may impair the Firewall Security.

For further discussion of the dynamic rules, please refer to the Firewall Security Manual.

## Firewall Logging

Firewall logging is an important and necessary firewall function; however, logging also uses system resources. The more logging rules which are inserted into the firewall rules table, the greater the amount of storage space and processor time needed to maintain accurate logs.

Though the primary method for fine-tuning the amount of information that gets logged is via configuration of the individual firewall rules, firewall logging in total can be enabled or disabled by checking or unchecking the **Firewall Logging** box in the Security Level dialog.

## Other Performance Issues

Aside from the number of observed connections, the creation of dynamic rules, and the logging preferences of the administrator, a number of other factors may also affect the performance of the firewall and the system on which it is running:

- Some individual rules require more system resources than others. Rules which consume excessive amounts of CPU or disk resources may need adjustment or removal in order to be viable. This subject is further detailed in the Firewall Security Manual.
- Features which use strong encryption, such as the IPSec plugin, are always CPU intensive; older or overloaded systems may not therefore have enough power to perform these tasks effectively.
- The **Assemble Packets** option in the **Intermediary** tab of the Firewall Properties dialog, which causes the firewall to defragment and analyze incoming traffic, is also CPU-intensive. For more information on this option, refer to "Fragmentation Control" in Section 4.4, "Other Firewall Properties."
- Improperly tuned Maximum Transmission Unit (MTU) and Maximum Segment Size (MSS) values may negatively impact network

performance and the amount of available bandwidth. For more information on these issues, refer to "Fragmentation Control" in Section 4.4, "Other Firewall Properties."

Note that on firewall machines which perform other duties in addition to firewall-oriented tasks, other processes on the system unrelated to the InJoy Firewall™ can also affect firewall performance.

## 8.5. Using Dynamic IP Addresses

Most commonly, firewalls are thought of as being run on computer systems with statically assigned IP addresses. However, some types of connectivity may instead rely on dynamic IP addresses.

The InJoy Firewall™ includes features designed to allow the Firewall to function properly when the external interface IP address is dynamically assigned.

### When Are IP Addresses Changed?

Users who use Point to Point Tunneling Protocol (PPTP), Point to Point Protocol over Ethernet (PPPoE) or DHCP to connect their firewall's external interface to the Internet will find that their addresses are subject to change, often without notice.

In some cases, users may also change the IP addresses of systems which normally have what is considered to be a static IP address.

In all of these cases, the InJoy Firewall™ offers features to automatically detect the changed IP address and update its configuration. Flexible configuration adjustments are necessary to ensure that the address transition is transparent and secure.

### Managing IP Address Changes

Depending on the used access technology, the InJoy Firewall™ detects the IP address change differently:

- **PPTP and PPPoE**
  The IP address of your Firewall PC is negotiated as part of the PPTP and PPPoE protocol. Any new IP address is automatically injected into your system and immediately activated.
- **DHCP and Manual IP Address change**
  When a new IP address is assigned through DHCP or via manual configuration, the InJoy Firewall™ tracks the IP address change by periodically checking the IP address of the physical network interface. By default, this check is performed every 30 seconds.

  To adjust the interval at which the network interface is checked, edit **config\gateway.cnf** using a text editor such as Notepad or Emacs and change the value of the **Rescan-IP** variable to the number of seconds the Firewall Server should wait between checks. For example, to cause the Firewall Server to check for a new IP address every two hundred (200) seconds, change (or add) the line to read:

```
Rescan-IP = 200,
```

Note that setting the variable to a value of zero (0) disables dynamic IP checking; when set to zero, if the IP address of the network interface changes for any reason, the Firewall Server will not detect the change.

After changing the **config\gateway.cnf** file, be sure to completely restart the Firewall Server.

### Script Execution at IP Address Change

When the InJoy Firewall™ discovers a change of IP address, it automatically executes the script **newip.cmd** (on Windows and OS/2) and **newip.sh** (on Linux).

These scripts are passed the new IP number as a parameter, allowing you to automatically update dynamic DNS servers and other configurations related to your dynamic IP number.

## 8.6. Firewall Packet Tracing

Firewall Packet Tracing is an important tool for observing activity that passes over a network interface. The InJoy Firewall™ provides for two kinds of packet tracing, quick packet tracing using the Firewall Server console and full packet tracing using a predefined firewall rule.

### Quick Tracing

Quick packet tracing is accomplished at the Firewall Server console. To enable quick packet tracing, press Shift-T (uppercase '**T**'). You will begin to see output on the firewall console supplying the following packet information:

```
Trace: OUT (after processing) (size 78) (MAC IF)
Trace:    source ip.: 207.212.1.252 (MAC 00.50.56.40.40.be)
Trace:    dest. Ip..: 207.212.4.36 (MAC 00.40.f4.0a.7d.23)
Trace:    payload...: prot(UDP) src_port(137) dst_port(137)
Trace:    result....: OK (Normal Packet) (15)
Trace: OUT (after processing) (size 78) (MAC IF)
Trace:    source ip.: 207.212.1.252 (MAC 00.50.56.40.40.be)
Trace:    dest. Ip..: 207.212.4.36 (MAC 00.40.f4.0a.7d.23)
Trace:    payload...: prot(UDP) src_port(137) dst_port(137)
Trace:    result....: Dropped by Firewall (128)
```

Notice that the word **Trace:** appears before each firewall console line which is output by the quick packet trace feature. Because the Firewall Server Console monitor mirrors the content displayed on the Firewall Server console, all of the output discussed above will also appear on the Firewall GUI activity log.

To disable (stop) quick packet tracing, press Shift-T once again.

### Full Packet Tracing

Full packet tracing is a more serious, more involved measure for tracing packet activity across the firewall. When full packet tracing is enabled, *all data* passing through the firewall network interfaces is saved and stored. This data can then be passed through an analysis tool later, in order to generate output fit for investigative purposes.

Full packet tracing requires disk space to match the amount of traffic entering and exiting through a network interface, for the amount of time that full packet tracing is to be enabled. Analysis of the stored data requires several

orders of magnitude more storage, as each packet generates a large amount of additional data.

Details for using full packet tracing follow:

1. To begin a full packet trace, open the desktop folder and the InJoy Firewall™ application folder. Then, select **IP Trace (Start)** from the **Packet Tracing** folder. This will create a file called packet.trc in your firewall's base install directory. This file will contain *all data* which passes through your firewall.
2. To stop packet tracing, leaving the trace file intact, select **IP Trace (Stop)** from the **Packet Tracing** folder.
3. To format the raw IP packet data for analysis and output it, use the **ipformat** command in the InJoy Firewall™ base install directory, supplying **-r** as an option and the **packet.trc** as an argument. In general, the output should be redirected to a text file:


The result of the ipformat command should result in the file dump.txt, which then includes nicely formatted IP packets:

```
------------------------- #:118 -----------------------
 IP:  Dest: 080.080.012.103    Source: 192.162.001.032
 ---------------------- IP HEADER --------------------
 IP:  Version: 4 Correct    Header Length: 20 bytes
 IP:  Type Of Service: 00
 IP:     000. ....  Routine
 IP:     ...0 ....  Normal Delay
 IP:     .... 0...  Normal Throughput
 IP:     .... .0..  Normal Reliability
 IP:  Total Len: 352 (x160) bytes        Id: 5308
 IP:  Flags: 4
 IP:     .1..       May Fragment
 IP:     ..0.       Last Fragment
 IP:  Fragment Offset: 000
 IP:  Time To Live: 128 sec     Protocol: 6
 IP:  Header Checksum: 8816
 IP:  No Options
 ---------------------- TCP HEADER ----------------------
 TCP:  Source Port: 1108  (Unassigned port)       Dest Port: 80  (Reserved)
 TCP:  Sequence #: 2656148865
 TCP:  Ack #: 2155937855
 TCP:  Offset: 20 bytes
 TCP:  Flags: 18
 TCP:     ..0. ....        Urgent bit Off
 TCP:     ...1 ....  <ACK> Ack bit On
 TCP:     .... 1...  <PSH> Push bit On
 TCP:     .... .0..        Reset bit Off
 TCP:     .... ..0.        Synchronize bit Off
 TCP:     .... ...0        Finish bit Off
 TCP:  Window: 64800      Checksum: 67E3
 TCP:  No Options
 -------------------------------- DATA ---------------------------------
 [0000] 47 45 54 20 2F 73 74 79    6C 65 73 68 65 65 74 73   GET /stylesheets
 [0010] 2F 77 69 6E 5F 69 65 5F    62 74 73 70 6F 72 74 65   /win_ie_btsporte
 [0020] 6E 2E 63 73 73 20 48 54    54 50 2F 31 2E 31 0D 0A   n.css HTTP/1.1..
 [0030] 41 63 63 65 70 74 3A 20    2A 2F 2A 0D 0A 52 65 66   Accept: */*..Ref
 [0040] 65 72 65 72 3A 20 68 74    74 70 3A 2F 2F 77 77 77   erer: http://www
```

```
[0050] 2E 62 74 2E 64 6B 2F 0D    0A 41 63 63 65 70 74 2D   .bt.dk/..Accept-
[0060] 4C 61 6E 67 75 61 67 65    3A 20 64 61 0D 0A 41 63   Language: da..Ac
[0070] 63 65 70 74 2D 45 6E 63    6F 64 69 6E 67 3A 20 67   cept-Encoding: g
[0080] 7A 69 70 2C 20 64 65 66    6C 61 74 65 0D 0A 49 66   zip, deflate..If
[0090] 2D 4D 6F 64 69 66 69 65    64 2D 53 69 6E 63 65 3A   -Modified-Since:
[00A0] 20 57 65 64 2C 20 32 30    20 4D 61 72 20 32 30 30    Wed, 20 Mar 200
[00B0] 32 20 31 31 3A 34 39 3A    31 36 20 47 4D 54 3B 20   2 11:49:16 GMT;
[00C0] 6C 65 6E 67 74 68 3D 31    33 30 33 0D 0A 55 73 65   length=1303..Use
[00D0] 72 2D 41 67 65 6E 74 3A    20 4D 6F 7A 69 6C 6C 61   r-Agent: Mozilla
[00E0] 2F 34 2E 30 20 28 63 6F    6D 70 61 74 69 62 6C 65   /4.0 (compatible
[00F0] 3B 20 4D 53 49 45 20 36    2E 30 3B 20 57 69 6E 64   ; MSIE 6.0; Wind
[0100] 6F 77 73 20 4E 54 20 35    2E 31 29 0D 0A 48 6F 73   ows NT 5.1)..Hos
[0110] 74 3A 20 77 77 77 2E 62    74 2E 64 6B 0D 0A 43 6F   t: www.bt.dk..Co
[0120] 6E 6E 65 63 74 69 6F 6E    3A 20 4B 65 65 70 2D 41   nnection: Keep-A
[0130] 6C 69 76 65 0D 0A 0D 0A                              live....
```

Note that full packet tracing is expensive, both in terms of disk space and research time; it should not be considered an everyday measure under most circumstances.

## 8.7. Creating a Firewall Watchdog

Because computing conditions are rarely perfect and a firewall is a very important part of the infrastructure of any network, it is often important to ensure that the Firewall Server is restarted should it stop unexpectedly for any reason.

In order to ensure that the Firewall Server automatically restarts, administrators of dedicated firewall systems should be sure to create a watchdog script from which the Firewall Server is started. This script simply calls the Firewall Server (named: gateway.exe) and, if the server exits, starts the server again immediately. For example, a Windows batch file to do this called **c:\ijfw\watchdg.bat** might contain:

```
C:\IJFW\GATEWAY.EXE
C:\IJFW\WATCHDG.BAT
```

This script simply starts the Firewall Server and, if the Firewall Server exits, calls itself once again, thus starting the Firewall Server, *ad infinitum*.

System administrators of more involved systems or configurations should add reporting and logging features to such a script to ensure that the status of the Firewall Server is known.

# Part IV
# Networking with the InJoy Firewall™

# 9 Setting up an Internet Gateway

This section is designed to help you to use the InJoy Firewall™ as a gateway machine for your own network. Among the topics discussed in this section are:

- Understanding Network Address Translation (NAT)
- Understanding Demilitarized Zones (DMZs)
- Steps necessary to create your own private network and connect it to the Internet using the InJoy Firewall™
- An example walk-through for creating a private network

Note that the content in this section is written with Windows users in mind. Because the InJoy Firewall™ is a multi-platform product, you may need to adapt the operating-system-specific information in this chapter to suit your own platform needs.

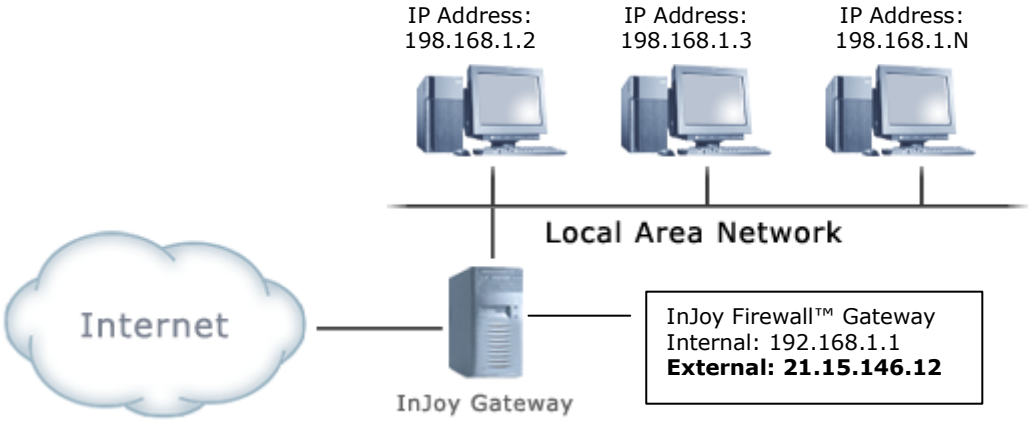
## 9.1. Using Network Address Translation (NAT)

As the number of hosts connected to the Internet has grown, the technology known as Network Address Translation (NAT) has grown steadily in popularity. NAT is used and supported by major equipment vendors such as Cisco, 3Com, IBM and many more. The InJoy Firewall™ also provides users with access to NAT functionality.

## What is NAT?

NAT is a TCP/IP networking technology that allows a network to access the Internet through a single public IP address. At the same time, all internal work-stations will appear as a single host to the outside world. When this occurs, the real IP addresses of the internal hosts are hidden; to computers on the public Internet, only the IP address of the NAT host is known.

The below figure illustrates how NAT on the InJoy Gateway PC is used to provide Internet access for the 3 internal PCs.




**Here is how the IETF describes NAT:**
"IP V4 Network Address Translation (NAT) has become an increasingly common function in the Internet for a variety of reasons. NAT is used to interconnect a private network consisting of unregistered IP addresses with a global IP network using [a] limited number of registered IP addresses. NAT is also used to avoid address renumbering in a private network when topology outside the private network changes for a variety of reasons. And, there are many other applications of NAT operation."

## What is NAT used for?

Though there are many possible uses for NAT, at present NAT is most often used to connect private networks which use unregistered network addresses to the public Internet. These network addresses are reserved for free, unrestricted use on internal networks in RFC documents 1597 and 1918. They include the following IP ranges:

- **Class A:** 10.0.0.0 through 10.255.255.255
- **Class B:** 172.16.0.0 through 172.31.255.255
- **Class C:** 192.168.0.0 through 192.168.255.255

In its most common use, NAT allows machines in these networks to share a single connection to the Internet while using standard Internet protocols.

NAT is not in and of itself a firewall; however, by its very nature of operation, NAT provides a measure of security for any network client using a NAT host as its gateway. This is true for two reasons:

- Because the IP address of the LAN client using a non-routable IP address, which is completely hidden from the outside world.

- Because on the NAT Gateway, the network interface connected to the public Internet is generally physically separated from the one connected to the internal network on the NAT host.

By using the InJoy Firewall's filtering capabilities in conjunction with NAT, you can provide Internet access to an entire network of machines over a single point of connectivity, and you can do so securely.

## NAT Compatibility Issues

Because NAT is a well-tested, largely transparent technology, there are very few compatibility issues between NAT and common Internet protocols. All of the following tools function properly with NAT:

- Web browsers such as Internet Explorer, Netscape, Mozilla, or Opera
- File Transfer Protocol (FTP) clients
- Standard e-mail clients such as Microsoft Outlook, Eudora, Pine, PMMail, The Bat, or Ximian Evolution
- Network News Transfer Protocol (NNTP) readers
- Chat technologies such as Internet Relay Chat (IRC), ICQ, or AOL Instant Messenger
- Peer-to-peer file sharing, such as Napster, Overnet, Morpheus, KaZaa, eMule or GNUtella
- TCP/IP network utilities such as ping, traceroute or telnet
- IPSec VPN software, in particular when the IPSec software – like the InJoy Firewall – supports the IPSec NAT Traversal feature.

A select few applications do not function well with NAT. These include:

- Network programs or utilities which do not use the TCP or UDP transport layer protocols, with the exceptions of ping and traceroute
- Microsoft NetMeeting
- Some streaming media or online entertainment applications

Because NAT hides the IP addresses of hosts on the internal network, network servers cannot be run on internal network hosts unless IP port forwarding rules are defined in the InJoy Firewall™ security plugin.

## InJoy Firewall™ NAT Configuration

The InJoy Firewall™ can operate either as a gateway machine with NAT enabled, or as a firewall-only host without making use of NAT. If you want to use NAT with the InJoy Firewall™ to provide a gateway for an internal network, you should check to ensure that the following are true:

- You chose to **enable IP forwarding** when installing the InJoy Firewall™
- Your current security level specifies "Outgoing NAT connections allowed" in its description and the Allow by Default item is checked in the Security Level dialog, **or—**
- You have created a firewall rule unblocking all ports above port 10,000 to allow NAT traffic on the firewall host

For details on enabling IP forwarding during the installation process, please refer to Section 2.3, "Graphical Installation." For details on setting a Security

Level or creating firewall rules, please refer to Section 8.3, ”Managing Firewall Security.”

## 9.2. Deploying a Small Network

For inexperienced network administrators, a checklist and step-by-step guide to using NAT for an internal network can be helpful. This guide should not be considered exhaustive, but is enough to configure a small internal network of the type commonly used with broadband ISP connections.

### A Small Network: Preparation Checklist

Before you can begin to actually deploy your small network, you must first make the following decisions and/or perform the following tasks:

- Ensure that each machine you wish to use on your internal network contains at least one working network interface card
- Ensure that the machine you wish to use as a firewall/gateway contains at least two working network interface cards

  **Note:** Two network interface cards are not always technically required in the gateway machine, but it is the recommended setup – as two NICs provide physical separation of the internal and the external networks.
- Obtain network cabling and a network hub with at least as many ports as you have machines (including the firewall/gateway host)
- Decide on an internal network address range (192.168.1.* for most users) and an IP address within that range for each machine
- Make a list of these addresses to help you keep track of them:

  Firewall/NAT Gateway – 192.168.1.1
  Host #1 – 192.168.1.2
  Host #2 – 192.168.1.3
  Host #4 – 192.168.1.4
  (etc.)

### A Small Network: Step-by-Step

Once you have made all of the necessary preparations, you can deploy your network. Network deployment will generally involve the following steps, which do not necessarily have to be performed in this order:

1. Install the InJoy Firewall™ on the firewall and configure it for use as a NAT gateway for your network. For details, please refer to “InJoy Firewall™ NAT Configuration” in Section 9.1, ”Using Network Address Translation (NAT).”
2. Configure each host on the internal network to use the static reserved IP address that you have assigned to it.
3. Configure each host on the internal network to use the firewall/gateway host’s IP address as its gateway address (gateway address is also known as the “default route” on some Operating Systems).
4. Configure each host on the internal network to use the host 1.1.1.1 as its Domain Name Service (DNS) server. This will cause all DNS requests to be forwarded to your ISP’s nameservers.
5. Connect all of the internal hosts and the internal interface of the firewall/gateway host to the hub.

6 Connect the external interface of the firewall/gateway host to the ISP, using DHCP, PPPoE or a static IP address as necessary

7 Start the InJoy Firewall™ server and reboot each host PC to ensure that changes to network settings have been made active.

Once these steps have been performed, the machines on the internal network should be able to communicate with Internet hosts transparently, as if they were directly connected to the Internet.

## 9.3. Network Deployment Example

Because a list of steps can sometimes be difficult to follow, this section walks through a small network deployment using specific numbers and showing the dialogs involved for illustration purposes. The characteristics of this network are as follows:

- The network will contain five hosts, the gateway and a single 8-port hub
- The Class C network 192.168.1.0 has been chosen as the IP address range for the network
- The gateway will have the IP address 192.168.1.1, while all other hosts in the network are numbered 192.168.1.2 through 192.168.1.7
- The ISP provides a broadband connection via Ethernet and DHCP

This scenario closely matches those of many home networks being serviced by xDSL, Cable or other types of broadband connectivity.

### Configuring Windows Network Interfaces

Several of the steps in the following sections discuss the configuration of network interfaces in Windows. The dialog used to configure network interfaces in Windows 2000 can be reached by following these steps:

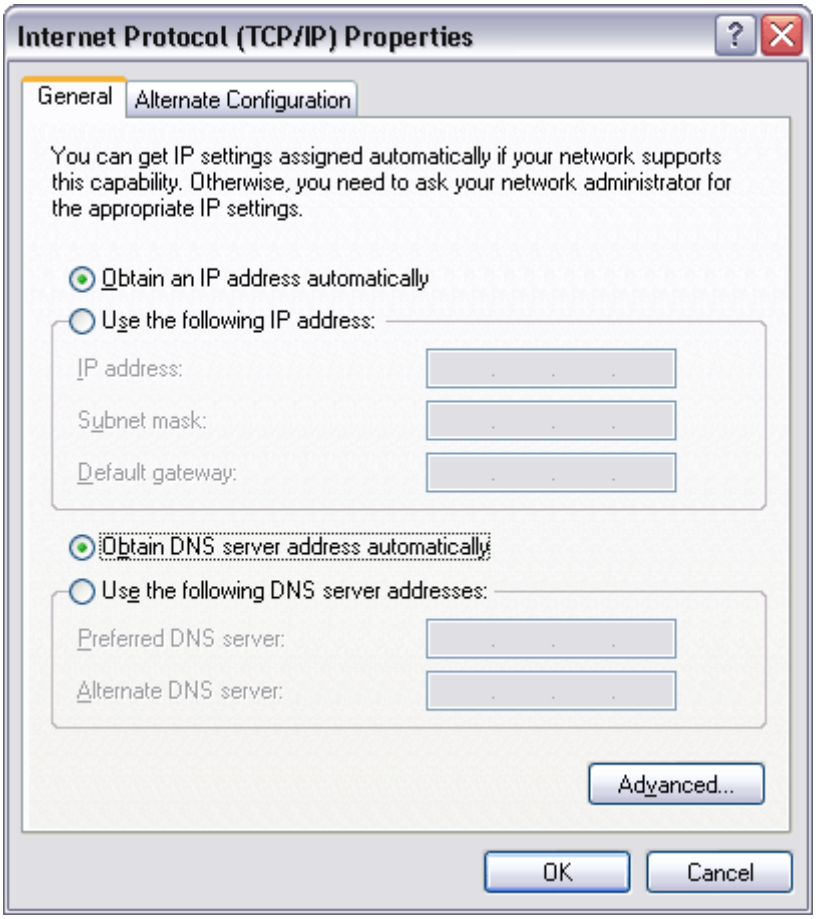
1 Click on **Start, Settings, Control Panel** to open the Control Panel.

2 Double-click on the **Network and Dial-up Connections** icon to open the Network and Dial-up Connections dialog.

3 Right-click on the icon representing the external network interface and select **Properties** from the pop-up menu to open the Local Area Connection Properties dialog.

4 Select **Internet Protocol** from the list of components and click Properties to open the Internet Protocol (TCP/IP) Properties dialog.

Once you have reached the Internet Protocol (TCP/IP) Properties dialog, you can configure the network interface using the provided options:



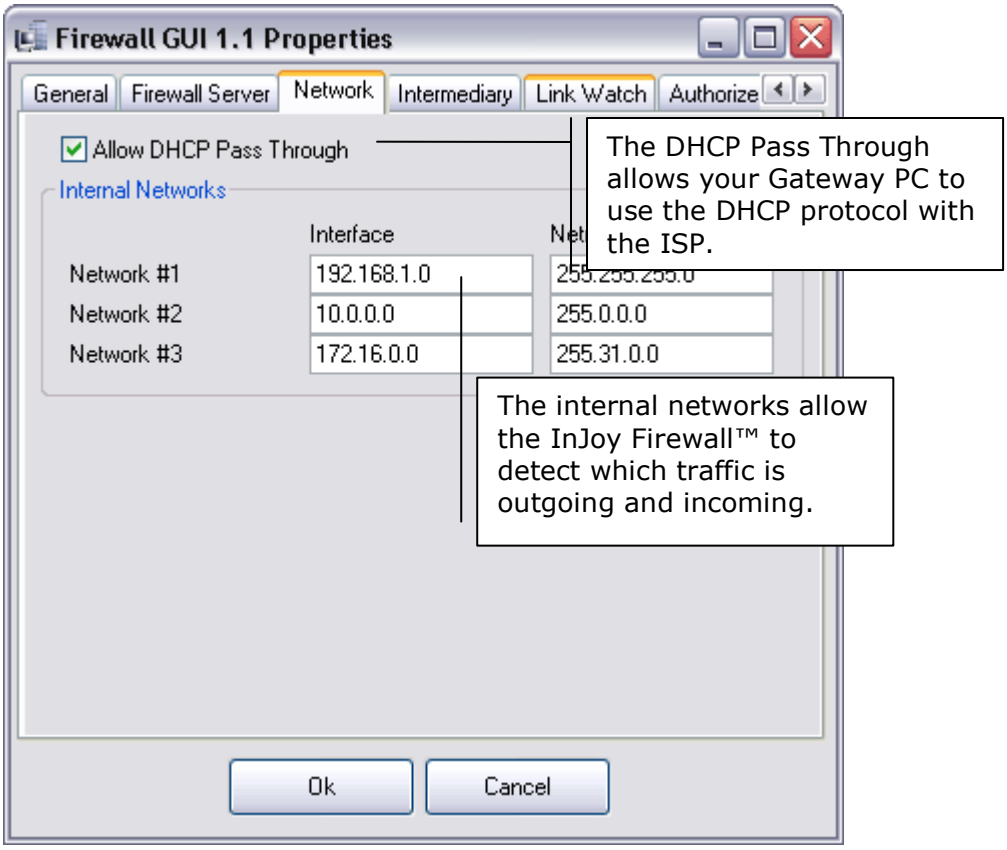

- Select **Obtain an IP address automatically** to cause Windows to configure the interface using DHCP, or—
- Enter values for **IP address, Subnet mask, Default gateway** into the upper half of the dialog
- Enter values for the **Primary DNS server** and **Secondary DNS server** into the bottom half of the dialog

After entering your changes, click **Ok** to save them.

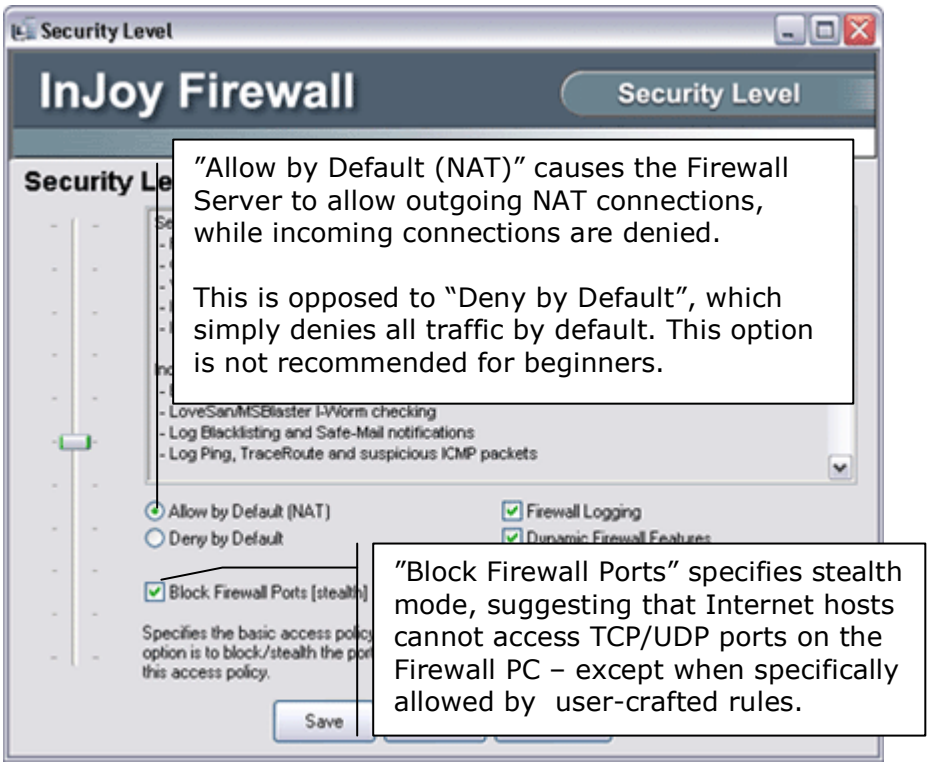
## Configuring the Firewall/Gateway Host

After installing the InJoy Firewall™ and taking care to **enable IP forwarding**, the following configuration tasks are carried out:

1 The default internal network 192.168.1.0 and netmask 255.255.255.0 are entered into the **Network** tab of the **Firewall Properties** dialog (see Section 4.2). No need to change the default value, however, if you were to use another internal address range, the internal networks should be changed to reflect that.




2 The default Security level five (5) is chosen in the Security Level dialog; this security level allows NAT traffic while blocking ports on the firewall/gateway host (from outside access).

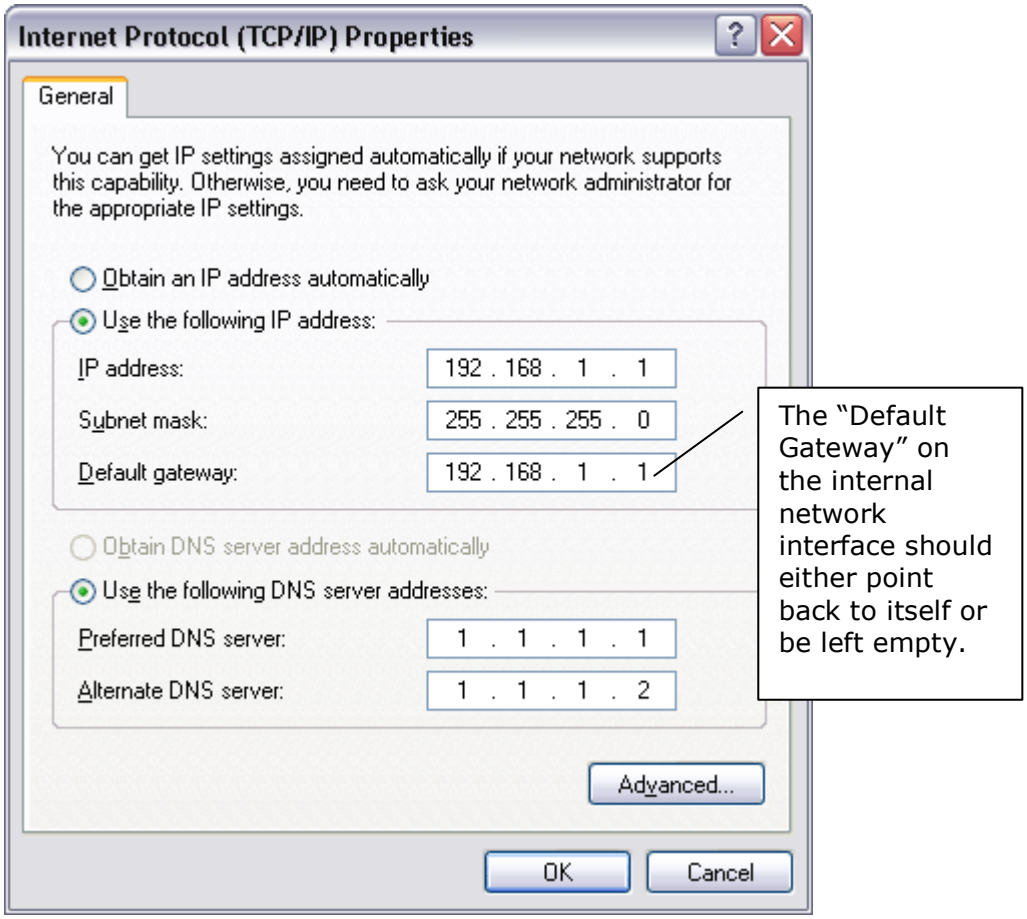



3 The external interface of the firewall/gateway host is configured to use DHCP to obtain its address, gateway and DNS information.

See previous section for a screen shot of the Windows TCPIP protocol settings.

4 The internal interface of the firewall/gateway host is configured with the following values:

192.168.1.1 (IP address)
255.255.255.0 (Subnet mask)
192.168.1.1 (Default gateway)
1.1.1.1 (Primary DNS server)
1.1.1.2 (Secondary DNS server)




5 The external network interface is connected to the ISP Ethernet interface. The internal network interface is connected to the hub.

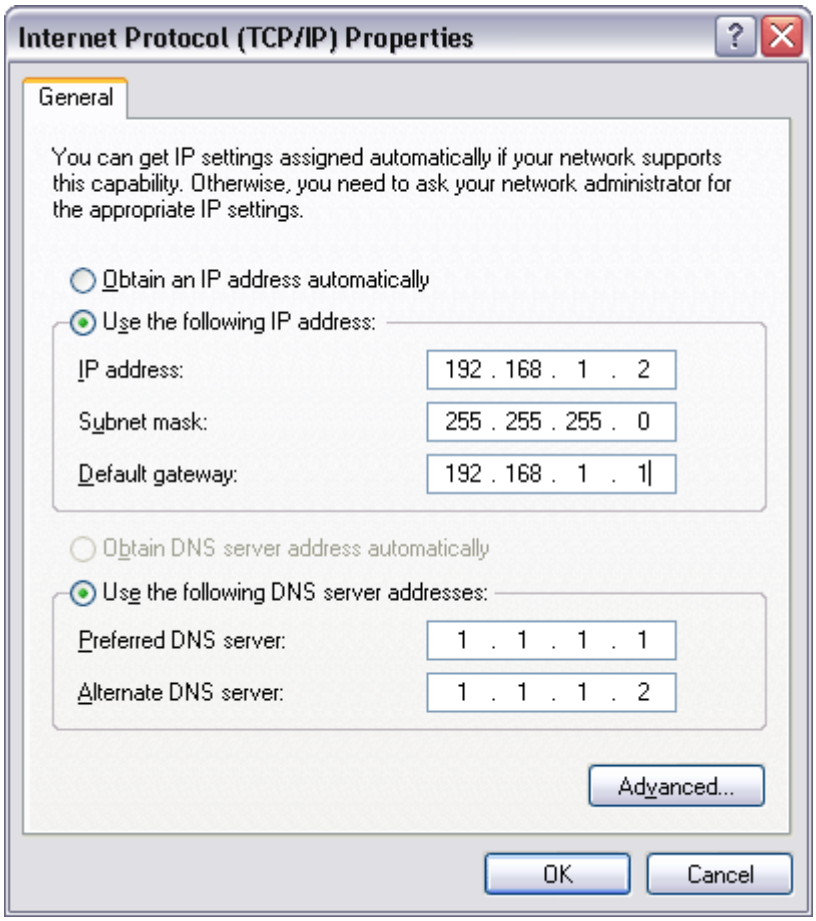
After these tasks have been completed, the firewall/gateway host is rebooted and the InJoy Firewall™ is started.

## Configuring the Internal Work-Stations

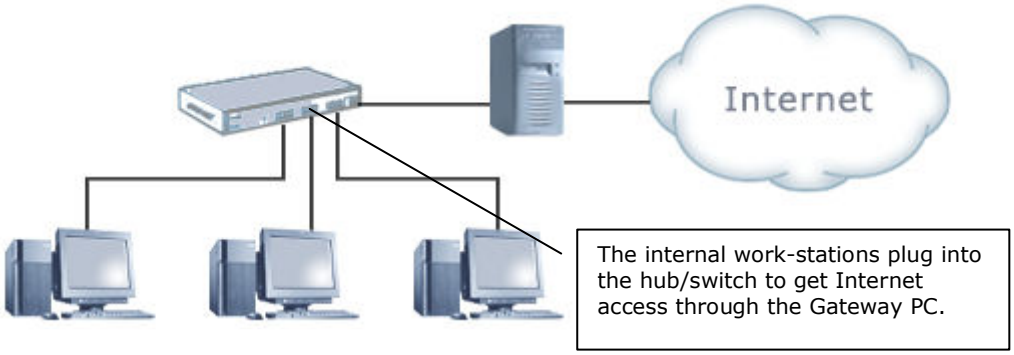
The process for configuring each internal network host is similar, but somewhat simpler. Keep in mind that each host has a different IP address, ranging from 192.168.1.2 through 192.168.1.7. The first host is documented in these steps:

1 The network interface of the first internal network host is configured with the following values:

192.168.1.2 (IP address)
255.255.255.0 (Subnet mask)
192.168.1.1 (Default gateway)
1.1.1.1 (Primary DNS server)
1.1.1.2 (Secondary DNS server)




2 The network interface of the first internal host is connected to the hub.




After these tasks have been completed, the network host is rebooted. These steps should be repeated for each host in the network (taking care to adjust IP address as necessary).

Once both the firewall/gateway host and the network hosts have been configured, the network should be functional. If the network hosts are able to

access the Internet, then the NAT functionality of the firewall/gateway machine is working.

## 9.4. Creating Demilitarized Zones (DMZs)

Sometimes it is necessary to provide NAT for some hosts on a network while passing traffic directly through to others. This is most often the case when some or all of the machines on a network have been assigned actual (non-private) IP addresses by an ISP, by IANA or by similar authorities.

To create and use a DMZ within your network, you must make three configuration changes to your firewall host:

- The IP address range must be supplied to the InJoy Firewall™ as one of its internal networks – specified in the InJoy Firewall™ properties.
- The IP address range must be specifically allowed in an InJoy Firewall™ rule in order to allow traffic for those addresses. The rule must allow traffic in both directions. For an example, refer to the **Internal-Server** rule in the **Rule Workshop**, **User Rules** dialog.
- The external network interface on the firewall host must be configured with alias IP addresses for each address in the address range. This is possible, by clicking "Advanced" in the TCPIP protocol properties.

### Supplying IP Addresses to the Firewall

IP address ranges for internal networks can be supplied to the Firewall Server using the Firewall Properties dialog. For details on opening and using this dialog, please refer to Section 4.2, "Verifying Internal Network Configuration."

For example, if your network has been assigned all unique addresses in the class C network **207.144.136.0**, you would enter 207.144.136.0 into the interface box and **255.255.255.0** into the netmask box.

### Adding Network Interface Aliases

To add address aliases to your external interface, simply add an additional range of additional IP addresses to the properties of the physical network interface connected to the outside world (i.e. to your ISP).

For example, in Windows 2000, this can be done by following these steps:

1. Click on **"Start | Settings | Control Panel"** to open the Control Panel.
2. Double-click on the **Network and Dial-up Connections** icon to open the Network and Dial-up Connections dialog.
3. Right-click on the icon representing the external network interface and select **Properties** from the pop-up menu to open the Local Area Connection Properties dialog.
4. Select **Internet Protocol** from the list of components and click Properties to open the Internet Protocol (TCP/IP) Properties dialog.
5. Click **Advanced** to open the Advanced TCP/IP Settings dialog.
6. In the **IP Settings** tab, click **Add** to open the TCP/IP Address dialog.
7. Enter the IP address range and netmask into **IP address** and **Subnet Mask** boxes.
8. Click **Add** and then **Ok** to save your changes.

Once you have added the necessary aliases to your external network interface, proxy Address Resolution Protocol (ARP) can properly function to allow your firewall host to transparently pass traffic to the hosts which have assigned public IP addresses.

## Security in the DMZ

By default, the NAT feature rejects all incoming traffic to the computers in the DMZ and accordingly, only traffic allowed specifically with firewall rules will flow to/from the DMZ.

# Part V
# References

# 10 Appendix A - Utility programs

## 10.1.Sync

The Sync tool can perform a variety of utility tasks and is therefore very useful when creating scripts and command-files that manipulate InJoy products without user intervention.

The Sync tool provides the following features:

- Re-read configuration of these plugins: Firewall, DHCPd, IPSec;
- Re-start or terminate the InJoy Firewall™;
- Dynamically activate or deactivate firewall sample rules and load them into production rules.

Note: Sync must be run from the base directory of the InJoy Firewall™ installation.

### Re-reading Plugin Configuration Files

| Parameter | Description |
|---|---|
| -firewall | Performs full reloading of the Firewall Security Plugin configuration and executes the following actions:<br>• flushes all logging and accounting files;<br>• closes all internal structures and queues;<br>• closes all current Safe-Mail proxy connections;<br>• re-reads configuration, performs validity checks and resolves DNS names in rules;<br>• initializes accounting and logging;<br>• initializes the Safe-Mail proxy. |
| -dhcpd | Performs full reloading of the DHCP Server Plugin and restarts the DHCP Server. |
| -ipsec | Performs full reloading of the IPSec VPN Plugin and executes the following actions:<br>• sends out ISAKMP Delete Notifications for every connected SA to ensure that SAs are cleared by the remote endpoints;<br>• re-reads configuration, does validity checks;<br>• initiates new IKE negotiations, as specified in the SAs. |

## Re-starting InJoy product

| Parameter | Description |
|---|---|
| -restart | Re-starts the InJoy Firewall™ product by performing full shutdown of all loaded plugins and the host application, then starting it again. |
| -kill | Shuts down the InJoy product. |

## Managing Firewall sample rules

The **firewall\features** sub-directory allows the Firewall Security Plugin to dynamically load special Firewall rules. This feature is useful for scripted activation of certain rules.

As the Firewall Plugin configuration is reloaded, rules found in the above mentioned folder are inserted at the end of the regular Firewall rules – i.e. after the rules specified in **firewall\firerule.cnf**.

| Parameter | Description |
|---|---|
| -on:<name> | Loads <name> rule file by copying firewall\samples\<name>.cnf to firewall\features\<name>.cnf and then reloads the Firewall configuration. |
| -off:<name> | Unloads <name> rule file by deleting firewall\features\<name>.cnf and then reloads the Firewall configuration. |

## Working with a Specific InJoy Firewall™ Instance

Additionally, the Sync tool can perform any of these tasks for any loaded instance of the InJoy Firewall™ through. For example, if you are running several InJoy Firewall™ instances (on several network interfaces), you will need to specify which InJoy product instance to work with, by using -inst parameter.

The instance number is equal to the device index, specified in **config\gateway.cnf**. To e.g. reload the configuration of the Firewall Security plugin, issue this command:


# 10.2.Ipformat

The Ipformat tool parses binary the representation of TCP/IP packets into text format, showing all the internal structures and headers of every packet. The following protocols are supported: IP, ICMP, ARP, TCP, UDP and DNS.

Ipformat can handle raw binary packet dump (the output of Firewall Plugin, with ”dump_bin” modifier in Log-Mask) and AIX/OS/2 IPTrace files, which in addition includes timing and MAC address information.

Ipformat writes to the screen, allowing users to redirect its output using the standard OS redirection features, like this:


### Usage

| Parameter | Description |
|---|---|
| -i [<name>] | Input filename specifies an AIX/OS/2 IPTrace file.<br><br>The **-i** parameter <name> specifies the file from which to read the packet input data. If not specified, the default file name **IPTRACE.DMP** is used. |
| -r <name> | Input filename specifies a file of raw IP packets (not Ethernet packets – i.e. no MAC headers!). The <name> parameter specifies the name of the input file. |

## 10.3.IPGate

The IPGate utility enables IP packets forwarding on a gateway machine. Port Forwarding is a feature that allows packets to be routed between different network interfaces. IP forwarding is usually enabled on machines that act as routers, NAT gateways, and similar.

Under Windows, IPGate modifies the following system registry key:

```
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter
```

Under Linux, IPGate modifies the following item under the proc file-system:

```
/proc/sys/net/ipv4/ip_forward
```

Under FreeBSD, IPGate modifies the following systole entry:

```
net.inet.ip.forwarding
```

Under OS/2, this tool is native.

### Usage

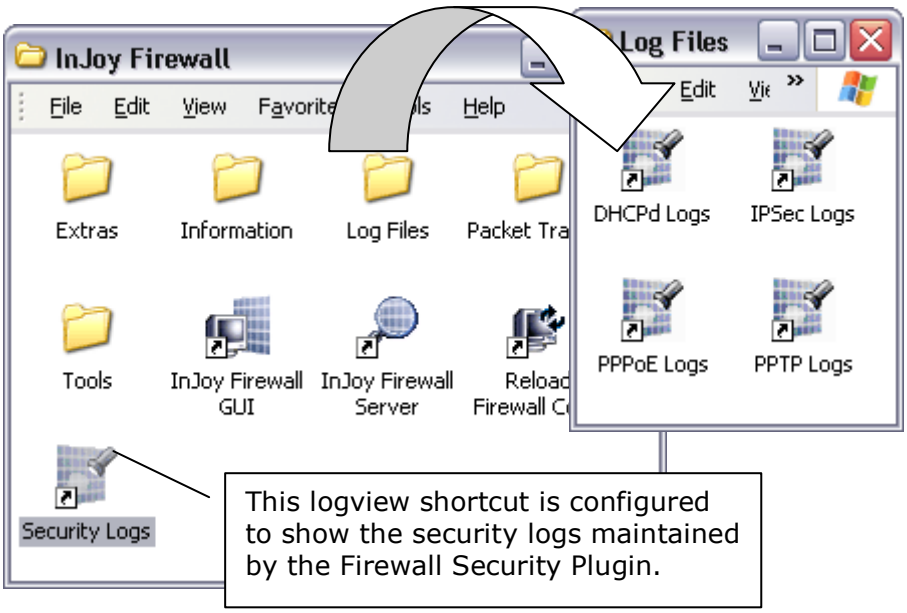
| Parameter | Description |
|---|---|
| On | Enables IP forwarding. Rebooting is required to activate the change. |
| Off | Disables IP forwarding. Rebooting is required to activate the change. |
| Check | Checks the current IP Forwarding setting and provides a choice to enable it, if it's currently "disabled" (supported on Windows only). Rebooting is required to activate changes. |

# 10.4.Logview

The Logview tool provides a user-friendly GUI interface for dedicated viewing the many log files maintained by the InJoy Firewall™.

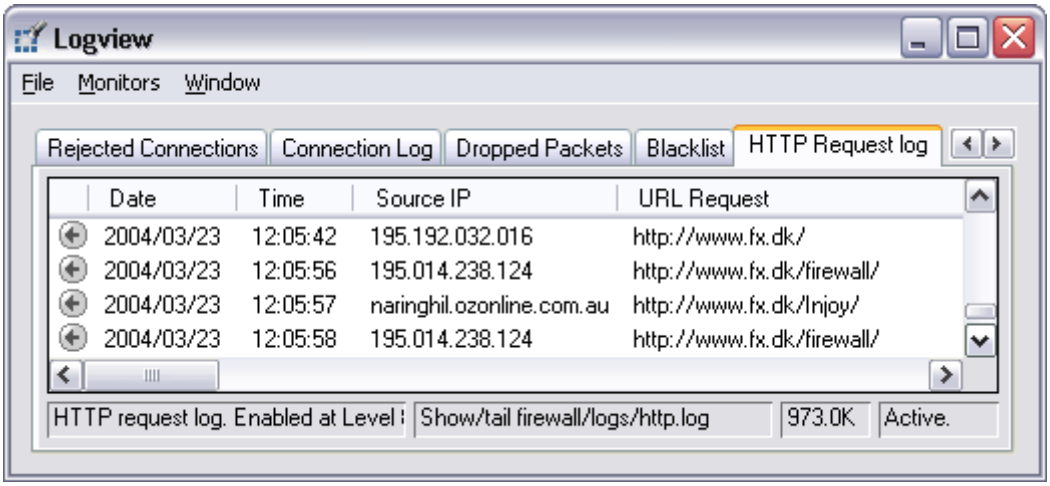
## Starting Logview

Logview is set up with pre-configured shortcuts in the InJoy Firewall™ desktop folder, allowing you to quickly find and monitor the logs you need.




## Using Logview

As you start up logview, you will see a row of tabs across the top of the Logview tool; clicking on a tab will show the log in question. You can use the scroll bar on the right side of the Logview window to scroll up and down while reading a log:




Viewing Security Logs in Logview is particular beneficial when viewing custom log files, created by your own Firewall rules.

If problems or questions arise which can not be answered simply by watching the GUI monitors, the firewall logs are the obvious next resource. It is suggested that users who are particularly concerned about security archive firewall logs for future reference.

The Logview tool works on files and can work locally or with network drives shared using the “file and printer sharing services”.

## Notices

Searching logs in Logview is possible only for the clear-text logs and not for the logs that are displayed as individual columns (in containers).

While Logview is introduced in this section, a full discussion of its possibilities is outside the scope of this document.

# 11 Appendix B - Summary of Configuration Files

## 11.1.General Properties

| Filename | Description |
|---|---|
| config\gateway.cnf | General settings of InJoy Firewall™, which include internal nets, remote GUI settings, enabled plugins, authorization info, and more...<br><br>GUI: **"File \| Properties"** |

## 11.2.Firewall Plugin Configuration

| Filename | Description |
|---|---|
| firewall\firewall.cnf | Common settings of Firewall Plugin: Safe-Mail, dynamic firewall, firewall stealthing, security levels are configured here.<br><br>GUI: **"Firewall \| Security Level"** |
| firewall\firerule.cnf | Contains firewall rules, crafted by the user.<br><br>GUI: **"Firewall \| Rule Workshop \| User Rules"** |
| firewall\shape.cnf | Contains Traffic Shaping / Bandwidth Management Firewall Rules.<br><br>GUI: **"Firewall \| Rule Workshop \| Traffic Shape"** |
| firewall\blacklst.cnf | Blacklist rules, updated both by the Firewall Plugin and the user. Updated automatically whenever a rule expires or when the Firewall Security Plugin blacklists an attacker.<br><br>GUI: **"Firewall \| Rule Workshop \| Blacklist Rules"** |
| firewall\whitelst.cnf | Whitelist rules (crafted by the user) to allow unconditional access to certain IP addresses. Rules are automatically removed when they expire.<br><br>GUI: **"Firewall \| Rule Workshop \| Whitelist Rules"** |
| firewall\features\ | Dynamically loaded firewall rules (using sync tool). Any .CNF file residing in this folder will be automatically loaded by the Firewall Plugin at start-up or as the result of reloading the Firewall configuration. |

| | |
|---|---|
| | GUI: None |
| firewall\rulelib\ | Pre-defined set of rules used in security levels. Generally, these files should not be edited, as they are overwritten with new version of the InJoy Firewall™.<br><br>GUI: **"Firewall \| Security Level \| Custom \| System Rules"** |
| firewall\samples\ | The sample rules demonstrate various Firewall Plugin features. They are not loaded by the Firewall – used only as a reference for the user.<br><br>GUI: "**Firewall \| Rule Workshop \| Sample Rules"** |

## 11.3.DHCP Server Configuration

| Filename | Description |
|---|---|
| dhcpd\dhcpd.cnf | Common settings of DHCP Server Plugin. Default route, DNS servers, interface netmask and other settings are specified here.<br><br>GUI: **"Firewall \| DHCP Server \| Properties"** |
| dhcpd\ip-pool.cnf | IP pools for the DHCP Server Plugin – sets of IP addresses that can be issued to DHCP clients.<br><br>GUI: **"Firewall \| DHCP Server \| Properties"** |

## 11.4.IPSec Configuration

| Filename | Description |
|---|---|
| ipsec\ipsec.cnf | Security Association Bundles (tunnel definitions) for the IPSec Plugin.<br><br>GUI: **"IPSec \| Tunnel Workshop"** |
| ipsec\vpn-auth.cnf | Authentication database for remote IPSec users (X-Authentication specifically), specifying User-IDs, Passwords and virtual IP addresses.<br><br>GUI: **"IPSec \| User Administration"** |
| ipsec\options.cnf | Common settings of IPSec Plugin, which include extended packet tracing, IKE Server start-up options and log files limit.<br><br>GUI: None |

## 11.5.PPPoE Configuration

| Filename | Description |
|---|---|
| pppoe\pppoe.cnf | PPPoE Plugin authentication, DNS-Servers, and other settings are configured here.<br><br>GUI: **"PPPoE \| Properties"** |

## 11.6.PPTP Configuration

| Filename | Description |
|---|---|
| pptp\pptp.cnf | PPTP Plugin tunneling settings.<br><br>GUI: None |

# 12 Appendix C - Configuration Attributes

The InJoy Firewall™ receives its general configuration from a plain text configuration file.

This configuration file can be edited manually or via the InJoy Firewall™ GUI ("**File | Properties**").

## 12.1. Firewall Properties

This section provides a quick reference of **config\gateway.cnf** configuration attributes and their possible values.

### Licensing Information

| Field | Possible Values | Description |
|---|---|---|
| Name | Alpha-numeric string | Authorization name. |
| Code | Alpha-numeric string | Authorization code. |

### Plugins State

| Field | Possible Values | Description |
|---|---|---|
| PPPoE | Enabled<br>Disabled | Defines the state of PPPoE Plugin. |
| PPTP | Enabled<br>Disabled | Defines the state of PPTP Plugin. |
| IPSec | Enabled<br>Disabled | Defines the state of Firewall Plugin. |
| DHCPd | Enabled<br>Disabled | Defines the state of DHCPd Plugin. |

## Internal Network Information

| Field | Possible Values | Description |
|---|---|---|
| DNS-1<br>DNS-2 | IP Address<br>(or leave empty) | Specifies the DNS servers to use for DNS forwarding.<br><br>Internal workstations can use 1.1.1.1 and 1.1.1.2 as their DNS servers and DNS requests (to 1.1.1.1 and 1.1.1.2) will automatically be forwarded to these DNS servers. |
| Internal-Net-1<br>Internal-Net-2<br>Internal-Net-3<br>Internal-Net-4<br>Internal-Net-5<br>Internal-Net-6<br>Internal-Net-7 | IP Address<br>0.0.0.0 | Together with Internal-Netmask-n, these configuration attributes specify the internal networks behind the Firewall (typically from the reserved range of 192.168.x.x, 10.x.x.x, etc).<br><br>Specify 0.0.0.0 to disable (not use) an internal network. |
| Internal-Netmask-1<br>Internal-Netmask-2<br>Internal-Netmask-3<br>Internal-Netmask-4<br>Internal-Netmask-5<br>Internal-Netmask-6<br>Internal-Netmask-7 | Netmask | The netmasks of the internal networks. |

## Identd Proxy Settings

Identd is an authentication server, mainly used by IRC and FTP servers to authenticate incoming connections. The proxy forwards incoming Identd requests to the respective clients on the internal network.

| Field | Possible Values | Description |
|---|---|---|
| Identd | Enabled<br>Disabled | The state of Identd Proxy. |
| Identd-User | Alpha-numeric string | If incoming identd request is destined to the firewall machine, Firewall responds with this user-id. |

## GUI Server Settings

| Field | Possible Values | Description |
|---|---|---|
| GUI-Server | Enabled<br>Disabled | The state of the GUI Server. |
| GUI-Password | Alpha-numeric string or encrypted password | The password of the GUI Server. Avoid storing it in clear text. Use GUI to encrypt the password.<br><br>Encrypted passwords are prefixed with a **-** character. For example:<br><br>`GUI-Password = "-74132bbcc98b00",`<br><br>Non encrypted passwords can be entered as they are. For example:<br><br>`GUI-Password = "rubberduck".` |
| GUI-Port | Valid TCP port number | TCP port number on which the GUI Server runs. |

## Link Watch

| Field | Possible Values | Description |
|---|---|---|
| Link-Watch | Enabled<br>Disabled | The state of the Link Watch. |
| Link-Watch-Interval | Numeric value | The number of seconds between each ping request. |
| Link-Watch-Host | Hostname<br>IP Address | Name or IP Address of the host to ping.<br><br>Note: be sure to select reliable ping host which is not offended by many ping packets. |

## Fragmentation Settings

| Field | Possible Values | Description |
|---|---|---|
| Fragment | Enabled<br>Disabled | Enable to have fragmented IP packets de-fragmented prior to firewall processing and fragmented again (using the MTU value, described below) as they leave the firewall. |
| MTU | Numeric value, not greater than 1500 | The MTU (Maximum Transmission Unit) specifies the maximum size of the TCP/IP fragments generated. Whereas the default value of 1500 is generally acceptable, a smaller value (e.g. 1400) should be using for packet enlarging protocols, such as PPPoE, PPTP and IPSec. |
| MSS-Adjust | Numeric value, smaller than MTU | Tweak the Maximum Segment Size (MSS) to force hosts to exchange smaller TCP data packets. Smaller packets prevent MTU related problems, such as non-fragmentable 1500 byte packets trying to pass through 1492 PPPoE pipe. Disable to let the TCP/IP stack set the MSS (typically 1460). |

## Miscellaneous Settings

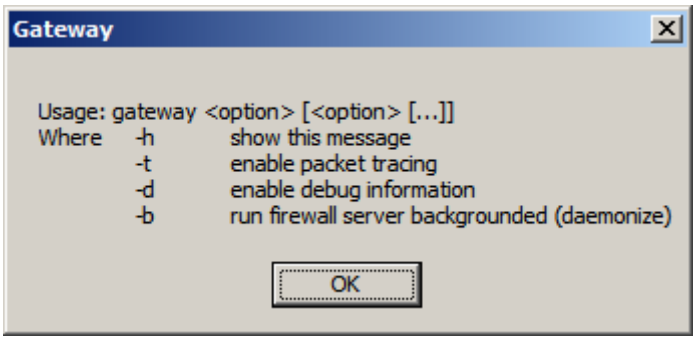
| Field | Possible Values | Description |
|---|---|---|
| Device-Index | Numeric value | Specifies the interface index on which firewall runs. While it is not possible to switch between interfaces from the GUI, you can use "fxinst –A –w" to change the current firewall interface from command-line. |
| Rescan-IP | Numeric value<br>0 | The interval in seconds between checking the Firewall network interface for a new IP address. The smaller the value, the sooner the Firewall will recognize a new interface address.<br><br>Use 0 to disable interface scanning. |
| Firewall-Directory | Name of existing directory under InJoy Firewall™ directory | Name of existing directory, containing Firewall Plugin configuration data. |
| OS2-SMC-Fix | Enabled<br>Disabled | SMC 8417T (10Base-T, SMC8000 driver) NIC can give TRAP 0E's on OS/2 under heavy load. Enable this workaround if you use this card.<br><br>Valid only on OS/2. |
| DHCP-Hole | Enabled<br>Disabled | Enable this option to allow your ISP/router to assign the IP address via DHCP protocol. If enabled, access to UDP port 68 on your system is allowed. |
| Priority | Numeric value in range 1..100 | Specifies the priority of InJoy Firewall™. |

# 13 Appendix D - Command Line Parameters

## 13.1.InJoy Firewall™ Server

When the Firewall Server is started without any command line parameters, it will appear normally in a window on the desktop.

If the Firewall Server is started with the **–h** parameter, it will list the possible command line options – as shown below:



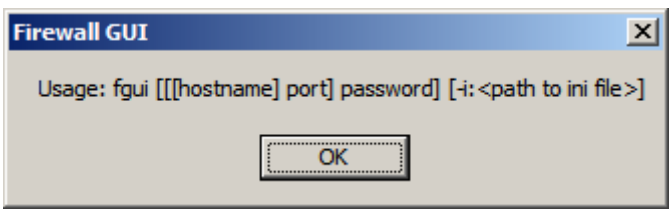

You may read more about the **–t** option (”enable packet tracing”), which is a feature that can also be toggled directly in the Firewall Server, in section 8.6 ”Firewall Packet Tracing”.

For more information about the **–b** option (”run firewall server backgrounded”), refer to section 3 ”Starting and Stopping the Firewall”.

## 13.2.InJoy Firewall™ GUI

If the Firewall GUI is started with no command line parameters, it will attempt to connect to the local Firewall Server – using shared memory. If multiple Firewall Servers are started locally, the GUI will list them and allow the GUI administrator to select a Firewall Server to control.

If the Firewall GUI is started with the **–h** on the command line, it displays the most common command line options – as shown below:




- The **hostname** is the DNS host name or the IP address of the remote Firewall Server. This parameter must be specified in order to connect to a remote Firewall Server.

- The **Port** is the TCP port number to connect to; i.e. that of the Firewall Server Remote GUI support. If the port number is omitted, the Firewall GUI defaults to 3333.
- The **Password** is the secret with which the Firewall GUI authenticates itself with the Firewall Server. If it is omitted, the Firewall GUI will prompt you to enter a password.
- The **"Path to ini file"** allows you to specify the location and file name of the special ".ini" file that controls the look & feel of the Firewall GUI. The default ".ini" file is fgui.ini, which will be loaded at GUI startup and changes relevant to the fonts, colors and window positions are also saved to this file. By specifying another ".ini" file, you can override the use of fgui.ini, making it possible to start multiple GUIs, each with its own individual appearance.

## Other GUI Parameters

In addition to the parameters listed in the above dialog, the Firewall GUI also accepts the following command line parameters:

- **-remote** indicates that the Firewall GUI is to connect to a remote Firewall Server and the GUI Administrator should be prompted for the remote IP address, and the password.
- **-#**, where **#** is a device-index. When the Firewall GUI runs locally on the same machine as the Firewall Server, it connects to a shared memory segment to obtain statistics. Each shared memory segment (there is one for every Firewall Server) is identified by the device-index of the network card the Firewall Server is installed to. An easy way to identify the device-index of a Firewall Server is by opening the **logs\status.gw** file and look for the **Instance: #** line. The value specified in place of the #, is the device-index.

The Firewall GUI parameters are described in greater detail in section 3.3, "Starting the InJoy Firewall™ GUI" and in chapter 5, "The User Interfac".

## Example

Command line parameters are typically used when the Firewall GUI must connect to a remote Firewall Server.

For example, to connect the Firewall GUI to a Firewall Server running at softdev.com, use this:

# 14 Appendix E – Using Multiple NICs

Installing multiple InJoy Firewall™ instances is necessary on a PC that has multiple insecure network interfaces. This is typically the case if more than one of the PC's network interfaces will be external (i.e. connected to the Internet).

## 14.1.Installing Multiple Firewalls

While the information in this section may contribute to the overall understanding, the information is only fully valid for the Windows platform. For other Operating Systems, please refer to the platform specific README files.

### Installing Multiple Firewall Servers

To install an additional copy of the InJoy Firewall™, simply run the InJoy installer multiple times. With each installation, take care to install into a different directory for each network interface.

For example, for a machine with two external network interfaces to protect, run the installer twice, installing into two directories with informative names:

- **C:\IJFW-NIC1** for the instance of the InJoy Firewall™ to be run on the first network interface.
- **C:\IJFW-NIC2** for the instance of the InJoy Firewall™ to be run on the second network interface.

If necessary, you can install as many copies of the InJoy Firewall™ as you have available network interfaces.

### Binding to a different network adapter

During Firewall installation, the installed Firewall instance is linked to the network adapter of choice. You may change this binding later, in one of the following ways:

1. **Completely re-installing the InJoy Firewall™**
   This method is recommended if you during installation selected secure mode for the driver (i.e. "BLOCK all IP traffic"). Full uninstallation and installation is required to alter the security setting for a specific network adapter.
2. **Manually changing the configuration file**
   This method requires editing the InJoy Firewall™ configuration file and it provides an easy way to quickly re-arrange which Firewall that binds to which network adapters.

To manually link an instance of the InJoy Firewall™ to a specific network adapter, follow these steps:

1. Visit the base directory of the firewall installation, for example, C:\IJFW-NIC1\ for the first network interface.
2. In the InJoy Firewall™ base directory, load the file **config\gateway.cnf** into a plain text editor such as Notepad or Emacs.
3. Edit the value of Device-Index to reflect the number of the physical network interface on which this instance of the firewall should run. For example, for the second physical network interface you'd edit the Device-Index line to read:

```
Device-Index = 2,
```

4. Save your changes to the file and exit your text editor.
5. Restart the InJoy Firewall™.

Repeat these steps for each instance of the InJoy Firewall™ that you have installed.

Notice the Device-Index can **only** be reliably determined from a previous installation or through careful experimentation.

## 14.2.Starting Multiple Firewall Servers

In order to start multiple instances of the InJoy Firewall™ Server, you must have performed a multiple firewall installation and followed the additional configuration steps required.

To start each instance of the Firewall Server, simply visit its base directory and start it by typing:

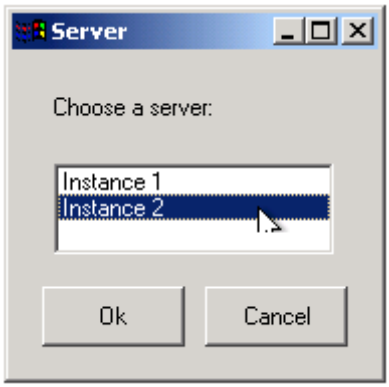

When started this way, the firewall service process will automatically retrieve the configuration information from the configuration files in its own base directory, including the number of the physical network interface to which it should connect.

## 14.3.Managing Multiple Firewall Servers

Several instances of the InJoy Firewall™ Server can be installed and running simultaneously on a single system. This is often the case on machines with several external network interfaces.

## Starting the GUI on Multi-Firewall Machines

When you start the Firewall GUI on a host that is running several instances of the Firewall Server, the Server dialog will appear. This dialog asks you to connect the Firewall GUI to a particular Firewall Server instance.




To finish starting the Firewall GUI, select the Firewall Server instance you want to manage and click **Ok**. To manage both Firewall Servers at once, simply launch the Firewall GUI a second time; two Firewall GUIs will then appear on your desktop, one for each running Firewall Server.

## Multi-Firewall GUIs at the Command Prompt

When several instances of the Firewall Server are running on a single machine, you can cause the Firewall GUI to immediately connect to a particular Firewall Server by supplying the number of the running Firewall Server as an interface as a command line option.

For example, if InJoy Firewall™ Servers were running on both the network interfaces of the Firewall PC, the following command would cause the Firewall GUI to connect to the Firewall Server that operates on Device-Index 2:


This technique can be combined with the **-i** option, so that the Firewall GUI can be instantly connected to a particular Firewall Server and particular appearance. The following command would cause the Firewall GUI to connect to third Firewall Server instance, using the appearance profile called nic3look.ini:


By creating desktop folder icons to execute commands of this type, GUI administration of multiple local firewalls can be streamlined.

**Acknowledgement**

We wish to express our gratitude to the many individuals who have contributed their energy, ideas and time towards the creation of our products.

**We would like to thank (in no particular order):**

- Beta testers - We wish to thank our many beta testers for ideas, advice and, of course for bug reporting.
- Clients/Users - We would like to thank all our clients for your excellent feedback and patience throughout the development of this latest, major update.
- Partners/Affiliates - Thanks to our affiliates and partners for working closely with us in bringing the optimal software to the streets.
- DBSoft - We wish to thank Brian Smith for his open-source contributions to the software.
- Silvan Scherrer - For your particular long-time support and product ideas.
- Law Offices of Charles Lee Mudd Jr. - For the excellent legal representation in the US.

And of course, without the hard work and dedication of the productive F/X staff, neither company nor product would have come into existence.