

# WaterRoof User Manual

v 2.2

This is a small user manual for WaterRoof. Please note that you may find useful to look also at contextual mini help windows in WaterRoof. Click (?) wherever possible to open a small help. Please note: this manual is aimed at people who already know what a firewall is.

## WATERROOF MAIN WINDOW: FEATURES AND TOOLS

When started **WaterRoof** will show its authentication popup window. Enter your password and click "OK" to authenticate. You can access almost every **WaterRoof** tool and feature from the main window. You can close it, but if you want you can re-open the main window from the top bar menu "Window".

Main window buttons:

Click **[Static Rules]** to open Firewall Static Rules Table window.  
 Click **[Dynamic Rules]** to open Firewall Dynamic Rules Table window.  
 Click **[Bandwidth Manager]** to open Dummynet Traffic Shaping - Bandwidth Manager.  
 Click **[NAT Setup]** to configure NAT and port redirection.  
 Click **[Net Connections]** to list active network connections and selectively block or limit bandwidth.  
 Click **[Net Processes]** to list active network files.  
 Click **[Ready Rule Sets]** button to open Rule Sets window.  
 Click **[Configuration Wizard]** button to open the Wizard.  
 Click **[Firewall Logs]** button to open Logs window.  
 Click **[Logs Statistics]** button to open Logs Statistics window.  
 Click **[IP Reverse and Whois]** to open IP Info window and make a reverse/whois query.  
 Click **[Network Interfaces]** to show available network interfaces.

## TOOLS

You may access tools from the top menu-bar.

### • Import/Export rules

Import or export current rules/pipes/queues configuration to/from file. When exporting you will be prompted for a filename. This is the ipv4 configuration file. The ipv6 configuration file will be saved in the same position with the "\_v6" suffix added to the ipv4 name. When importing the configuration files you will be prompted to choose the ipv4 configuration file. The ipv6 configuration file must have the same name of the ipv4 file with the suffix "\_v6", and must be in the same directory. If the ipv6 configuration file is not found WaterRoof may prompt an error, but the ipv4 rules will be loaded without problems.

### • Startup configuration

Save/Delete/Restore rule set activated at boot time. This set is saved in /etc and can be recalled directly from the static rules window.

### • Startup script

Instal/remove startup script. It is used to activate at boot ipfw rules, pipes, queues, forwarding, logging and nat. Please note: startup configuration for Mac OS X 10.4 and 10.5 is different. WaterRoof will automatically choose the right one, but please take care if you do edit it manually.

### • Firewall logging

enable/disable ipfw logging. Confirm twice if you want to start logging at system boot.

Please note: enabling log at boot in Mac OS X 10.5 may be unnecessary and may cause the system to log and error (stray process) in /var/log/system.log. This issue has no effect a part from logging the message.

### • Flush rules and pipes

Delete all active ipv4 and ipv6 rules and pipes. Rule 65535 is active by default and can't be deleted.

- **Enable/Disable IP Forwarding**

Enable or disable IP Forwarding (sysctl). Useful for example in dual-homed firewalls. You have also the option of keeping this setting active upon reboots. This option is activated automatically when running NAT.

- **AppFirewall Debug**

Experimental debug tools for the Leopard appfirewall. Use at your own risk. It is advisable to setup the Leopard Application Firewall using only OSX System Preferences.

## USEFUL MAN PAGES

You can display some useful man pages in a easy readable format from the **WaterRoof** menu "Help".

## ADD, MOVE, EDIT, REMOVE, UPDATE AND SAVE IPFW STATIC RULES

Static Rules Windows shows active ipv4 and ipv6 ipfw static rules. Use the "ipv6" button to switch between the 2 modes.

In Static Rules Window:

- Click [ + ] button to add a new firewall rule.
- Click [ - ] button to delete selected firewall rule.
- Click [ ↑ ] button to move up selected rule
- Click [ ↓ ] button to move down selected rule
- Click [ ✎ ] button to edit selected rule
- Click [ ↻ ] button to update rules table.
- Click [ Ø ] to reset packets and bytes counters
- Click [ ✕ ] button to flush current rules, pipes and queues
- Click [ ♥ ] button to restore rules from startup configuration
- Switch [ ipv6 ] button to change ipv4/ipv6 mode.

- **deleting a rule**

Click [-] button to delete selected firewall rule. You can't do multiple selection. You can't delete rule number 65535.

- **moving a rule**

Changing rules order affects firewall behaviour. You should take care when moving rules.

Click [↑] button or [↓] button to move UP or DOWN selected rule. You can't move rule number 65535. You can't move a rule below rule number 65535.

- **modifying an existing rule**

Double-click a rule to open the modify panel. You can't modify rule number 65535.

- **adding a new rule**

Click [+] button of the main window to open the new rule panel. Enter your rule parameters then click [Add] to add the rule, [Cancel] to return to main window, [Show Shell Command] to popup the shell command that would be issued when adding. Beware: you should have more than one rule with the same number. When adding a new rule, **WaterRoof** will set up the number for you. You can change it in the New Rule window, or you can also change it later by moving up or down the rule in the main window rule list table. Do not forget to specify ipv4 or ipv6 protocol for the rule.

## STATEFUL FIREWALL: SHOW DYNAMICALLY CREATED IPFW RULES

Dynamic rules are created automatically by ipfw. If you want to know more about dynamic rules, please refer to the ipfw man. You can also display the help on the Dynamic Rules window. Displaying dynamic rules has mainly a debug/testing purpose. Please note that stateful operations in firewall are potentially subject of denial of service attacks. Check ipfw man pages for more info. Click the "?" to show a new window with a brief explanation of dynamic rules. You have also the option to activate a predefined rule set with stateful operations enabled. With this rule set you can see how ipfw generates new temporary rules dynamically.

To activate the new set click "Activate example configuration". Please note: doing so will flush your current

rules. Remember: you can export your actual rules configuration for backup purposes at any moment. To see ipfw generating dynamic rules just try a few connections to lan/remote servers. For example try to connect to a web site and see how ipfw will create specific rules to allow ip traffic from/to this server's ip address. Click "Update List" to update rules list.

- **Update List**

Updates dynamic rules table.

- **Include expired**

Include expired dynamic rules when listing. Dynamic rules usually stay alive for a few seconds. If you want to see expired rules just check this option and update the list. Beware: including expired rules may increase parsing time consistently.

## MANAGE IPV4 BANDWIDTH

Bandwidth management is available only for ipv4. Traffic shaping for ipv6 is not available in Mac OS X. Dummynet Bandwidth Management Limiting bandwidth in Mac OS X is quite easy: we just need to set up a pipe and decide which packets will go through this pipe. Traffic passed through the pipe will be limited by pipe configuration. A pipe has 3 main options: Bandwidth (Kbit/ s), Delay (ms) and Slots (1-99).

If we need to do more fine-tuning then we can use queues. Please read man pages for more information about dummynet queues. You can also use the wizard to set a simple bandwidth rule, then you can edit and test it. You may also try rule sets.

- **Pipes table**

In this table are shown pipes and related rules, bandwidth, delay and slots.

- **Add new pipe**

Click [+] to open this window. Use this form to create a new pipe. Pipe number is determined by **WaterRoof**, but you can change it. You can also specify a rule number (but you can change this number moving the rule in the main window), a number of slots (1-99), delay in milliseconds, bandwidth in Kilobits per second (Kbits/s). You can choose to add a rule but you can also do it later in the static rules window.

Click [Add] to add the new pipe. A new pipe will be shown in the pipe list table. If you close the panel you will find the new rule in the main window rule table.

- **Queues table**

In this table are shown queues and related rules, weight, pipe and slots.

- **Add new queue**

Click [+] to open this window. Use this window to define a queue and a rule. Queues can have more rules, and they will be shown together in the queue window.

- **Modify existing pipe settings**

Double-click a pipe in the table to open the modify panel. You can modify pipe bandwidth, delay and slot. If you want to modify pipe rule arguments please use the main window.

- **Delete pipe**

Click [-] to delete selected pipe.

## NETWORK CONNECTIONS

Net Connections window shows active ipv4 and ipv6 network connections. Use the switch to select v4 or v6 connections. Select a connection and click "Block selected connection" to popup the "Connection Inspector". Use it to block selected connection or to limit bandwidth. You can modify rule number and bandwidth (in Kilo bits per second).

## NETWORK PROCESSES

Net Applications window lists active ipv4 and ipv6 network file and their connections.

## NAT - NETWORK ADDRESS TRANSLATION AND PORT REDIRECTION

NAT Setup allows you to configure NAT daemon and port redirection. You may need to activate NAT if you want to share a single internet connection between more LAN computers . You can also use this and other features to setup a complete and working dual-homed firewall with OS X. Port redirections GUI makes it more easy... Easier than Mac OS X Server! ;-)

BEWARE: **WaterRoof** NAT Setup DOES NOT WORK on Mac OS X Server. Not yet. For Mac OS X Server users there is a nice free solution called NATural. Try it.

- **NAT options**

set NAT interface and options, then save configuration. The default location is /etc/nat.conf . Click "Default" to activate a configuration with default options used in Mac OS X Server 10.4.8

- **Enable/Disable NAT auto start**

Use this options to launch NAT daemon at boot time, keeping your options and port redirections. You can use this options

only while NATd is running.

- **Start/Stop/Restart NAT**

Controls NAT daemon.

- **Port redirection**

Use the form to add port redirections. This is the place where you set "exported services"; for example if the host is acting as a dual homed firewall, port redirections will allow you access your LAN's computers services from the internet.

Complete the form then click "Add port redirection". The record will be added and the configuration file will be automatically saved. Remember: to activate new port redirections you must restart NAT. If restarting does not work, try to stop NAT and then start NAT.

## FIREWALL LOGS

- **Enable firewall logging**

Select this option from the "Tools" menu in top bar menus. When logging is enabled ipfw logs connections matching log rules. IPFW logging is set with sysctl variable net.inet.ip.fw.verbose set to 1. Please note: Click the ? button to see a small how to about solving logs problems with **WaterRoof**. .

You have the option to keep this setting at boot time.

- **Disable firewall logging**

Disable logging.

- **Show Firewall logs**

Show firewall log entries in /var/log/appfirewall.log. You can filter output with a string.

- **Real-time logs**

Open logs in a terminal window. New logs records will be displayed in realtime. Log file is /var/log/ipfw.log

## LOGS STATISTICS

- **Raw Statistics and Graphic Statistics**

In the Logs Window you can filter output with a string and you can also show raw statistics based upon deny/allow state, blocked/passed source/ destination IPs, protocols, interfaces. Graphic statistics generates a detailed html report using fwanalog and analog. You can save results to desktop. You can fine tune Graphic

statistics preferences in order to speed up the procedure. You can specify which report section you want to include in your logs.

## REVERSE AND WHOIS

### IP Info window

Enter a valid IP public ipv4 address and click "Reverse" to get its DNS record (if any); Click "Reverse & Whois" to get DNS record and whois database record (if any). Beware: whois servers tend to deny multiple queries from the same host in short periods of time. Please don't flood whois servers.

## LEARN HOW IPFW WORKS WITH PREDEFINED RULE SETS

Rule Sets are 7 groups of rules each one with a special purpose. Select the set from the popup menu to read the description. You can modify set options if any, and then change the rule number. Some set consists of more than one rule; rules will be added with steps of 10 or 100. The rule number proposed by default is the first available number before the last rule (number 65535). Each rule set description is self-explanatory; just add the ruleset and look at the main rule table to see what has been added. Rule Sets are intended to be examples for the unexperienced user. If you want to add more specific rules you should add them manually using the [+] button in the static rules window of **WaterRoof**. If you want to delete a bandwidth pipe added by the "Limit Bandwidth" Rule Set, you must use the Bandwidth Manager.

You should test how ipfw works adding rule sets and modifying them. Remember: you can save ipfw rules/pipes/queues at any time, in order to backup it or to make your own rule sets. Use the "Tools" menu to export and import rule sets.

**WaterRoof** has also a "special" rule set called "Startup configuration".

This set is special because it is activated at boot time if the startup script is installed. But you may also create a "Startup configuration" without activating it at boot time. You may recall your "Startup configuration" at any time clicking the 'heart' button in the static rules window.

## THE WIZARD: LET WATERROOF DO IT FOR ME !!

The Wizard will help you set a simple firewall configuration from scratch. Anyway if you want to use a more easy firewall frontend you should try NoobProof. NoobProof is a free open-source firewall tool for Mac OS X 10.4 and 10.5, developed by HanyNet.Com. For more information please go to <http://www.hanynet.com/noobproof>. There you can also find a comparison between WaterRoof and NoobProof features.

The WaterRoof Wizard should be used by unexperienced users because it is very easy to understand how it works. Please note that starting the Wizard will flush all current rules and pipes to prevent unexpected behaviour when mixing rules.

\*\*\* The Wizard will NOT teach you what a firewall is, how networking works and how to stay safe... It is just "a way to start up". Understanding networking is a complex matter, you can't accomplish it using an application wizard. \*\*\*

When you end Wizard configuration you can add/remove/move rules to change firewall behaviour. The Wizard will set a predefined set of rules to obtain a medium security level. The Wizard is quite self-explanatory. Start it and

see. The configuration process is divided into 3 steps:

- 1) *select which local services you want to share with others;*
- 2) *select which remote services cannot be accessed by this computer;*
- 3) *enable bandwidth limits for web or mail or p2p traffic to this computer.*

Select options from popup menus and click "Add this rule" to add a new rule. You can add many different rules changing popup values and clicking again "Add this rule". This is true for all 3 configuration steps.

Beware: when you start the Wizard your rules will be flushed. Please do a backup copy of your rules using the "Export rules to file.." option in **WaterRoof** "Tools" menu.

## HOW TO SAVE RULES AND LOAD THEM AT SYSTEM BOOT

- Verify your ipv4 rules and pipes and ipv6 rules;
  - Go to menu *"Tools"* -> *"Startup Script"* and select *"Install Startup Script"*;
  - Go to menu *"Tools"* -> *"Rules Configuration"* and select *"Save to startup configuration"*;
  - To enable firewall logging go to menu *"Tools"* -> *"Firewall Logging"* and select *"Enable Firewall Logging"*;
- confirm twice if you want loggin to be enabled at system boot.

Thank you for using **WaterRoof** !!

©2009 hanynet.com

by **Hany El Imam**

*hanynet.com • Mantova • Italy*

*www.hanynet.com  
hany@hanynet.com  
hanymac@gmail.com  
hany@IRCnet #mac.it*

**YOU CAN DONATE USING PAYPAL TO hany@hanynet.com . THANK YOU.**

WaterRoof is freeware and open source software. GPL license applies.  
dedicato a mio padre.