PFLists

User Guide

hanynet.com

Welcome.

This is a free tool developed for personal purposes.
Its source code and binary bundle are available for free at my web site.
If you like it just mail me and tell me how happy you are.
If you don't like it then mail me and tell me what should I add or remove in order do to meet your needs. I'll do my best.
If you are incline you can support me with a small donation.
This software comes under the terms of a license which is not a license but a point of view. Basically you can do whatever you want with this code. You have no limits of any kind.
Please note: the use of this software may completely destroy your data, your mac, your house, your life. You are responsible for what you do, so take care.

Enjoy !

Hany El Imam
hanynet.com

ABOUT FIREWALLS

PFLists is not a firewall. Your Mac already features three built-in firewalls:

- **ALF**
- **PF**
- **IPFW**

ALF is an application firewall, while both PF and IPFW are network firewalls.
ALF can be configured using System Preferences “Security” pane.
PF and IPFW do not have a default graphic interface shipped with OS X, so they can be configured only using the shell terminal. Using the terminal is the favourite choice by most system administrators.

To configure PF and IPFW without using the shell terminal we must use a graphic interface (frontend) from third party software makers.

PFLists is a frontend for PF
it is inspired by the old Server Admin’s firewall tool shipped with old Mac OS X Server releases. PFLists requires OS X 10.7 or newer. If you want a more powerful PF frontend please have a look at IceFloor, a free and open source firewall frontend of OS X available at
www.hanynet.com.

PFLISTS ADDRESS GROUPS

The first important things to understand are the **Address Groups**.
Address Groups are containers. You assign different parameters to those containers in order to obtain a set of rules to pass or block incoming and outgoing connections.

Each PFLists Address Group features four parameters:

1) Name
2) Addresses
3) Allowed services
4) List

• Adddress Group's **Name**

Each group must have a unique name. Name must not contain white spaces or special characters. Please use only letters, numbers, - and _ .
Click the "+" button below the Group column to add a new group.

• Address Group's **Addresses**

Each group may contain a list of addresses. They can be IP addresses, network addresses or both. Each group may contain only one address, or many addresses. A group can also be empty.
Network addresses must be in CIDR notation, for exampe 192.168.2.0/24.
You can add addresses to a group importing them from a text file or manually.
Click the "+" button to add addresses to selected group.

• Address Group's **Allowed Services**

Each group may contain a list of allowed services. Services can be added to the selected group using the "+" drop down menu.
You can add as many services as you need to all groups.
Group allowed services list can also be empty.

• Address Group's **List**

There are 2 lists: "**inbound"** and "**outbound"**.
Address Group "_outbound" belongs to the "outbound" list. All other Address Groups belongs to the "inbound" list, including your custom groups.

PFLISTS DEFAULT RULESET

When you start PFLists for the first time, it will create a default ruleset.
The ruleset will not be effective until you start the firewall.

The default preset is made of four special Address Groups:

1) _any
2) _blacklist
3) _outbound
4) my_local_network

These groups are divided into 2 lists: “**inbound**” and “**outbound**”.
List “outbound” contains only “_outbound” Address Group.
List “inbound” contains all other Address Groups.

• Group _any

Group _any represents all possible ipv4 and ipv6 addresses. Think of it as the whole Internet including your local network.
This group cannot be deleted.
You can’t add or remove addresses to this group. This group contains only 2 addresses: 0.0.0.0/0 (meaning “all ipv4 addresses”) and ::/0 (meaning “all ipv6 addresses).
You can add and remove services to this group. By default, this group only has “Essential system services” assigned.
All inbound connections from group _any will be blocked except inbound connections to allowed services.

• Group _blacklist

Group _blacklist represents a list of untrusted addresses. All connections from/to those addresses is blocked.
This group cannot be deleted.
This group is empty. You can add addresses to _blacklist group to block them. Addresses belonging to this group are blocked so you can't add services to this list. The only thing you can do with this group is to add or remove addresses. You can leave the group addresses list empty if you don't need a black list. Both inbound and outbound connections from/to blacklisted addresses will be blocked.

• Group my_local_network

Group my_local_network represents the local network, for example your home network. The first time you launch PFLists, it will try to guess the local network CIDR address, and will create the default ruleset with group my_local_network. This group contains only one address record, your network address. For example 192.168.1.0/24
Service list include a small list of common services like Documents sharing, iTunes, iPhoto, usb printer sharing, Game center.
Group my_local_network is special only for the reason that it is created automatically by PFLists the first time you launch it.
Anyway my_local_network it's a normal group: you can delete it, you can add and remove addresses, and you can add and remove services. All inbound connections from group my_local_network will be blocked except inbound connections to allowed services.

• Group _outbound

Group _outbound is used to apply outbound filtering rules. Default PFLists configuration assigns “All Services” to this address group. This means that outbound connections are not filtered. If you want to enable outbound filtering you have to remove “All Services” from “_outbound” group, and add as many allowed services as you need. Your Mac will be able to connect only to allowed services.

Default preset behaviour

Using default preset your mac firewall will:

• **ALLOW** inbound connections from the whole Internet to your Mac’s Essential System Services;

• **ALLOW** inbound connections from your local network (home, work, wifi) to your Mac’s shared documents, iPhoto/iTunes shared libraries and shared usb printers. Nothing else.

• **BLOCK** all other inbound connections from everyone to your Mac’s services.

• **ALLOW** all outbound connections from your Mac.

INBOUND AND OUTBOUND CONNECTIONS

From your Mac's point of view a connection initiated by your Mac is an outbound connection.
A connection initiated by a remote host and targeting your Mac is an inbound connections.

For example if you open Safari and you type a URL you are initiating an outbound connection. This connection starts from your Mac's browser and targets a remote hosts, in this case a web server. Obviously the server will reply to you and send you html web pages. This is an outbound connection reply.

If your boss connects to your Mac's shared documents from a his computer, then (from your point of view) he is initiating an inbound connection to your Mac. Your mac will answer with an inbound connection reply.

So there are 4 types of connections:

- from your Mac to a remote host:
    - 1) **outbound connections**
    - 2) **inbound connections replies**
- from a remote host to your Mac:
    - 3) **inbound connections**
    - 4) **outbound connections replies**

PF firewall rules do pass or block inbound and outbound connections.
Inbound replies and outbound replies are automatically passed using states for TCP protocol and using timeouts for UDP protocol and are not affected by rules.

PFLists “Firewall” tab lists all Address Groups, as previously described.
Use the popup button to switch between **inbound** and **inbound** lists.
Please note: both inbound and outbound lists are active; use the popup button to choose which one you want to see or edit. Every preset includes both inbound and inbound lists.

• **inbound** list

The “inbound” list of Address Groups is the one you need to configure in order to protect your Mac from unwanted remote connections. There are 3 default Address Groups in “inbound” list: _any, _blacklist, my_local_network. You can remove or add new Address Groups as described in this guide.

• **outbound** list

The “outbound” list of Address Groups consists in one group: _outbound.
You can’t add or remove groups from this list. Here you configure outbound filtering. The default setting is to allow all kind of outbound connections. If you want to restrict access to the Internet from your Mac then you have to modify the Allowed Services list for _outbound Address Group: remove “All services (tcp,udp)” service, and add as many services as you need.

CREATE A CUSTOM RULESET

The default PFLists configuration may or may not suit your needs. So you have the opportunity to modify the default PFLists ruleset using PFLists interface. Before doing it, you should do a backup copy of the default configuration.

- **Backup your configuration**

From PFLists menu bar select “File” menu and click on “Export PFLists configuration”; give the file a name and save it. Keep it for future use. This is the correct way to backup configurations, but you can also use PFLists Presets to manage your collections of configurations. For example you may need to switch between presets if your networking environment is subject to change.

- **Modify existing Address Groups**

Now it’s time to create a custom ruleset modifying existing groups and creating new ones. Each group of addresses will be able to connect only to the services assigned to this group.

Start modifying existing groups: _any, _blacklist, _my_local_network .
To add services to a group you have to select it from the drop down menu “+”.
To remove a service from a group you have to select the group, select the service in Allowed Services column, then click “-” button below the Allowed Services column.

• **Create new Address Groups**

You can create new groups and assign them as many addresses and services as you need.
Groups can also contain a single address and a single service.
Groups with empty address list or with empty allowed services list will be ignored.
The same addresses can be put in different groups.
The same service can be assigned to different groups.
Group order, addresses order and services order do not matter.

• **Special group _any**

The group _any is special: services assigned to group _any will be available to everyone, and this may expose your services too much. Be careful adding services to _any group.
Be also careful about the “Essential System services” which is assigned to group _any by default: this service allows DHCP address lease. If you are using DHCP you should not remove this service.

• **PFLists Services Database**

PFLists has a default list of services. You may access this list when adding a new service to an address group using the drop down menu. This database of services can be modified. You can add or remove services from the list. Click the ✎ button below the “Allowed services” column to open PFLists Services Database and modify it.

• **The “All Services (tcp,udp)“ special service**

As you may have seen, the first service in Services Database window is “All services”. This is a special service, it represents “all possible services running on your Mac”. If you trust a specific IP or network, then create a group for this IP and assign “All services” to its Allowed Services list. The trusted IP will be allowed to connect to your Mac with no restriction.
This service is a special service: you can add it and remove it from groups Allowed Services list, but you can’t delete it from Services Database.
All services in Services Database (exlcuding the first one) can be deleted. You can also add custom services. If you want to restore the default PFLists Services Database click button “Restore default services list”.

• **Interaction between Address Groups**

If a specific IP address is allowed to connect to a specific service, but this IP is also contained in _blacklist group, then it will be completely blocked.
Group _blacklist takes precedence over all other groups.
An IP can connect to a service if it is allowed to do it at least one time thru your whole PF ruleset.

START AND STOP THE FIREWALL

Select “Firewall” tab. The ON/OFF button status and its label will tell you if PF firewall is enabled or disabled. Click on the button (and confirm) to start / stop the PF firewall. If PF is enabled then the “Apply” button will be available (clickable).

You can modify your PFLists ruleset while PF is running and while PF is stopped. Everytime you do modify it, the PFLists configuration will be saved, but PF rules won’t change until you click “Apply”. Otherwise, when you click “Enable selected preset” in Presets tab, both configuration and running PF rules will be updated at the same time.
Please do backups or new presets of your settings before making any changes.

If PF is enabled and you modify PFLists configurations then you have to **click “Apply” in order to apply changes**. Running PF rules will be updated and new rules will be active.
Please note: only connections starting AFTER clicking “Apply” will be affected by the new rules. Old connections will still be affected by the old rules. This happens because PF uses dynamic “states” to allow traffic.
If you want also old (active) connections to be affected by the new ruleset, you don’t have to click “Apply”. Instead you have to disable PF and re-enable it using the Start/Stop button in PFLists.

The first time you start PF within PFLists, startup script will be installed. PF rules will be loaded at system boot. If you don’t want to load PF firewall rules at boot you can uninstall startup scripts using PFLists menu bar.

PFLISTS OPTIONS

- **PF firewall logs**

Click “Show PF firewall logs” to open PF logs in Console.app. Click “Export PF firewall logs” to export PF logs to file. All blocked packets are logged.

- **Debug Window**

Click “Show debug window” to open the PFLists debug window.
Use debug window to show runtime PF rules and main PF configuration file. Click “Update” to update debug window contents in case you modify PF ruleset.

- **Preserve Apple PF anchor (com.apple)**

Check this option if you want to include Apple default PF anchor into your PF configuration. A PF anchor is a subset of rules. This particular anchor is needed by some OS X service. So check this option if you want to maximize compatibility with OS X. Please be aware that some rule included in this anchor may override rules set by PFLists. Uncheck this option if you want to have complete control over your PF firewall.

- **Enable Emerging Threats protection**

Emerging Threats is a free online service providing an updated list of well-known dangerous hosts. Check this option if you want PFLists to block all incoming/outgoing traffic from/to these dangerous hosts. If enabled, Emerging Threats list will be updated every 2 hours by your system. The update process is managed by launchd and occurs in background. You don’t need to keep PFLists open.

PFLISTS PRESETS

The first time you launch PFLists it will create a library of predefined PF presets. Each preset has a name and a description. Select “Presets” tab to see PFLists presets list. Each preset contains all information about a PFLists configuration.

The initial PFLists configuration is also included in presets list as “default”.

Predefined PFLists presets library can be modified. You can delete unneeded predefined presets and you can add new presets.

Add a new preset

Select “Firewall” tab and configure all your Address Groups with Addresses and Allowed Services.
Select “Options” tab and set you options.
Select “Presets” tab and click “+” button.
Provide a name and a description for the new preset. Please don’t use spaces or special characters for the name, and do not exceed 200 chars for the description. Preset description will be displayed in “Firewall” tab once the preset has been enabled.

Enable preset

Click “Enable selected preset” to enable selected preset. Please note: firewall must be ON in order to be able to enable a preset.

UNINSTALL PFLISTS

Select “Help” tab and click “Uninstall” to stop the PF firewall and remove all files installed by PFLists. The OS X firewall will be restored to factory default.

FILES INSTALLED BY PFLISTS

PFLists does not modify any OSX default file. It uses only its own set of configuration files. Here is the list:

- ***/Library/LaunchDaemons/com.hanynet.icefloor.plist***
  - this is the launchd script that kicks icefloor.sh script
- ***/etc/icefloor.sh***
  - this is the bash script that enables pf and logging
- ***/Library/Preferences/PFLists/***
  - this directory contains PFLists configuration preferences
- ***/Library/PFLists/***
  - this directory contains PF configuration files
- ***/tmp***
  - tmp directory is used by PFLists to store temp files
- ***/Library/LaunchDaemons/com.hanynet.pflists.emergingthreats.plist***
  - launchd script that kicks Emerging Threats update script
- ***/Library/PFLists/pflists_emergingthreats.sh***
  - Emerging Threats update script
- ***/LibraryPFLists/pflists.ettable***
  - PF table configuration for Emerging Threats

PFLISTS AND OTHER FIREWALLS

- **PFLists and network firewalls**

PFLists is a network firewall frontend. It is not safe to use more than one network firewall frontend at the same time. For example, if you installed IceFloor you should uninstall it before installing PFLists.
WaterRoof, NoobProof, IceFloor, DoorstopX are network firewalls.

- **PFLists and application firewalls**

You can safely use a network firewall together with an application firewall.
The “firewall” you find in OS X System Preferences, for example, is an application firewall. It is called ALF, and is part of OS X, like PF. You can use the OS X System Preferences firewall together with PFLists. They do different things and they can act together. Little Snitch is another application firewall.
Remember:
1) a connection must be allowed by both firewalls in order to pass.
2) a connection will be blocked if at least one firewall blocks it.

That’s it.

Enjoy!

PFLists is free, open source and ad free. Please support free software development with a small donation, thank you.

PayPal donations may be addressed to:
hany@hanynet.com

Bitcoin donations may be addressed to:
16UvmZcqEEYT5gYrTaGrh82d12726fQi5x

PFLists concept and code by **Hany El Imam**

www.hanynet.com

hany@hanynet.com

Villa Saviola(MN) - Italy

credits:

Thanks to A. Lauzon and S. Kolins
Thanks to all beta testers and supporters


hanynet.com