PFLists

PF Firewall frontend for OS X

V 1.0

User guide

hanynet.com

ABOUT OS X 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.

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.

We developed also IceFloor, another free PF frontend, much more powerful and feature-rich than PFLists.
Use PFLists for basic PF setups, and use IceFloor for advanced networking needs.
You can also use IceFloor and PFLists together. More about this topic in a next chapter of this guide.

More info about IceFloor at

http://www.hanynet.com/icefloor

In the past hanynet.com has developed also WaterRoof and NoobProof, frontends for the IPFW firewall.
Since OS X 10.7 IPFW firewall has been deprecated. Now the default network firewall for OS X is PF, a much more flexible and powerful tool coming from OpenBSD, a free Unix-like operating system.

PFLists is a group-based firewall frontend inspired by the old Server Admin’s firewall tool shipped with old Mac OS X Server releases.

PFLISTS GROUPS

The first important thing to understand is the GROUP.
Each PFLists group features three parameters:

1) group name
2) group content
3) group services

• **Group 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.

• **Group content**

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.

• **Group services**

Each group may contain a list of allowed services. Services can be added to the selected group by double-clicking on service name in the Services Database window.
The Services Database window contains a set of predefined services. You can customize this list adding or removing services from the database.
You can add as many services as you need to all groups.
Group services list can also be empty.
Click the “+” button to add services to selected group.

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 ruleset is made of three special groups:

1) _any
2) _blacklist
3) _my_local_network

• 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.

• 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.

• 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.

With the default settings your mac firewall will:

ALLOW connections from everyone in the whole Internet to your Mac's Essential System Services;

ALLOW connections from your local network (home, work, wifi) to your Mac's documents, iPhoto and iTunes shared libraries, shared usb printers.

BLOCK all other connections from everyone to your Mac.

PFLISTS CUSTOM RULESET

The default PFLists configuration may or may not suit your needs. So you have the opportunity to modify the default PFLists ruleset and build a new ruleset.
Before doing it, you should do a backup copy of the default 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 it to create collections of configurations. For example you may need to switch between configurations if your networking environment is subject to change.

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 the group name and click the "+" button below the Allowed Services column. The Service Database window will open; you have to double click on a service name in order to add it to the selected group.
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.

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.

Please note: 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.

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”.

Please note: 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.

START AND MANAGE PF FIREWALL

Select “Firewall” tab.
The button on the right is the Start/Stop button.
The label above it will tell you if PF is running or not.
The button will change between Start and Stop, according to PF status.

The first time you launch PFLists, the PF firewall should be off. Click “Start” to start the PF firewall. PF will be activated, and PFLists will install startup scripts used to load PF rules at system boot.

Now PF firewall is active with PFLists ruleset; now you can quit PFLists. PF will stay active in background. Next time you reboot your Mac, PF firewall rules will be automatically loaded by the system in background. PFLists will not open, you don’t need to open it.

If PFLists has been started and you need to make some change to a running PF configuration you don’t need to stop PF: just make your changes in PFLists interface while PF is running, then click “Apply” to activate the new rules.

If you need to temporary stop PF then click “Stop”. Please note that if you stop PF, after next reboot it will be activated again.
If you want to keep your PF configuration installed but you don’t want to start PF at boot, then choose “Remove startup scripts” from PFLists “Firewall” menu in menu bar.

UNINSTALL PFLISTS

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

Please note that PFLists does not remove or modify any OS X system file.
PFLists uses its own set of configuration files and script which are completely independent from system files.

USE PFLISTS WITH ICEFLOOR OR OTHER PF FRONTENDS

When you start PFLists for the first time the PF firewall should be stopped. You can verify it in PFLists “Firewall” tab, above the Start/Stop button.
If PF is running, then probably you previously started PF manually or using IceFloor or using another PF frontend.

If so, then quit PFLists and open IceFloor and uninstall IceFloor from IceFloor menu bar.
Then reopen PFLists and click “Start” to install and start using PFLists.

If you don’t have IceFloor, then you can click “Uninstall” in PFLists “Firewall” pane. Doing so you will uninstall all PFLists file and also old IceFloor startup scripts. PFLists will then quit. Reopen it and click “Start” to install and start using PFLists.

You can also use PFLists and IceFloor together.
You can use PFLists to configure and start PF, and IceFloor to browse PF ruleset installed by PFLists, to monitor labels and tables and logs. Remember: if you activate IceFloor ruleset, PFLists ruleset will be overridden and viceversa. Please be careful when using IceFloor and PFLists together: you can use IceFloor to see logs and use Rules Browser to check rules, but you can't modify rules or apply IceFloor options.
If you set up PF using PFLists, then IceFloor can be used only as a monitor tool.

FIREWALL LOGS

All blocked packets are logged by default to /var/log/pffirewall.log
Select "Options" panel to show firewall logs using Console.app or to export logs to text file.
If you need numerical statistics and graphic statistic of your logs, you can use IceFloor.

CREDITS

PFLists code by Hany El Imam

www.hanynet.com

PFLists is free and open source. Source code is available at www.hanynet.com/pflists .

NLPL License applies, please see application menu and application bundle
You can find an on-line copy of NLPL at www.hanynet.com/nlpl

PFLists is available **for free**. If you want you can make a **small donation**.

PLEASE SUPPORT FREE SOFTWARE DEVELOPMENT
THANK YOU

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

Bitcoin donations may be addressed to: **16UvmZcqEEYT5gYrTaGrh82d12726fQi5x**

Please send me feature requests, bug reports and code contributions to
hany@hanynet.com

Grazie.

ENJOY !!!