IceFloor

PF firewall frontend

version 1.1

User guide

hanynet.com

Welcome to IceFloor

IceFloor is **not** a firewall.
IceFloor is a graphic interface for PF, the OS X firewall.
IceFloor let's you choose between two options:

1) for the beginner:

Use IceFloor **graphic interface** to configure PF settings. **Select services** to open, select **allowed hosts** (Action), select optional **black list** and **custom services**. Do everything from IceFloor interface, avoid editing PF configuration files manually. Do not use IceFloor "Manage PF rules" feature. Enable and disable the firewall clicking "**Enable PF firewall and install boot scripts**" and "Disable PF firewall and uninstall boot scripts". IceFloor will install a **custom subset of PF rules** and **boot scripts**. Rules will be immediately active and will be loaded at boot. Selected network services will be available to selected remote hosts, **all other services will be blocked**.

2) for the expert:

Use IceFloor "**Manage PF rules**" window to browse **PF rules tree** and to build your own **rules and anchors**. and to manually add and manage custom **PF tables**. Manage boot scripts PF status and **PF configuration** independently. Use the IceFloor built-in **text editor** to **edit configuration files**. You can also use the IceFloor rules manager to **modify, replace or delete rules** installed by IceFloor.

Both the beginner and the expert will be able to see, search and **parse PF log file**, looking at most **offensive remote hosts** and debug / test PF configurations with IceFloor's **port scanner**, connection **inspector**, and PF **states monitor**.

About PF and IceFloor

OS X 10.7 Lion comes with 3 built-in firewalls:
IPFW : the old Mac OS X network firewall, now deprecated
PF : the new OS X network firewall
ALF : the application layer firewall, configured in System Preferences prefpanes.

IceFloor is a **frontend for PF.** Its main purpose is to speed up and simplify PF configuration, tests, debug.
In the past, when IPFW was the default firewall in Apple systems, we developed 2 IPFW frontends: WaterRoof and NoobProof. The former was only aimed at system and network administrators, while the latter main purpose was easy of use.
With IceFloor we delivered a single application for both purposes. Starting IceFloor you are presented with a **list of services** and 3 possible **action** options: allow everyone, allow my LAN, allow a list of IP addresses. You can **activate the PF firewall** with a solid configuration in a few clicks.
But you can also start with the PF **rules tree browser**, and add your rules and anchors manually, manage tables and their contents, all in one window.
You can decide your **approach** to PF configuration.

PF is a much more complex tool than IPFW.
In order to be able to deal with PF logic you absolutely need to read manpages or **OpenBSD documentation**.
Despite that, you will able to use IceFloor to filter your network connections even if you don’t know what a manpage is.
This manual tries to help you.

This version of IceFloor is for clients only, it is not designed for OS X Server.
NAT and port redirection/forwarding is not yet supported. If you need to manage traffic on more than one network interface you must configure PF manually. The default rulesets installed by IceFloor are effective on all network interfaces except the loopback interface.
PF logging is enabled by default by PF boot scripts installed by IceFloor.
Blocked packets logging is enabled by default on PF configurations installed with IceFloor rulesets. You can manually add and remove rules or modify them to remove the “log” option if you need.
PF log file is /var/log/pffirewall.log

IceFloor needs **OS X 10.7 Lion** or later.
For older Mac OS X versions (with IPFW) please check WaterRoof and NoobProof at
www.hanynet.com

Open IceFloor

The beginner should start here.
The first window is the main IceFloor window.
This window is divided into 3 sections:

- service list
- action
- buttons

Service list

Your mac is running network services. For example if you enabled file sharing, or itunes sharing, you are running network services. If your mac is connected to a network then remote computers can connect to your services. This is possible in your home network, your office network or in public wifi areas.
If you don't want other computers to connect to your mac's services then the best solution is to stop those services. But this can be annoying and unsafe, as you may forget it.
Another solution is to use network filters. This means you may want to decide who is able to connect to your mac, using network filters.
In IceFloor, if you want to allow connections to a service you have to put a checkmark in its name.

Action

So you have decided which services you want to leave open. Now you can decide if everyone can access them or if you want to allow only someone. You have 3 options:

- **Allow everyone** = allow everyone (except blacklisted IPs, see later) to connect to my mac's selected services
- **Allow only local computers (LAN)** = allow only computers in my Local Area Network
- **Allow only a list of IP addresses (White List)** = allow only computers listed in the "White List" to connect to my mac's selected services.

If you choose option 3 then you may want to add IP to the White List.
White List is a list of IP addresses and/or subnets. Computers in this list will be allowed to connect to your mac's selected services.
Click "**Advanced options**" to open a new panel window: on the bottom of this new panel you will find the "White List" text field. Insert IPs and/or subnets address separated by white spaces.

If you choose option 3 and leave the White List empty, then no one will be able to connect to selected services.

Start IceFloor

Now it's time to activate the OS X firewall with those settings.
Click this button:

"**Enable PF firewall and install boot scripts**"

to:

- **enable** the OS X built-in PF firewall
- **load** and enable pf rules set (anchor) with settings taken from IceFloor interface
- remove old IPFW (WaterRoof and NoobProof) rules and boot scripts
- **install** boot scripts to start PF at boot and load PF rules

Now the OS X firewall is running. You can quit IceFloor. You don't need to run IceFloor anymore. Remember: IceFloor is NOT a firewall. The firewall is the OS X built-in PF and **runs in background**. The PF firewall runs even if IceFloor is closed.
Next time you reboot your mac, boot scripts will load automatically PF rules. You don't need to re-open IceFloor or to put IceFloor in login items.
You don't even need to log in. PF rules are loaded and active at system boot, also if it left at login screen with no users logged in.

Stop IceFloor

Use button "**Disable PF firewall and uninstall boot scripts**"
to:

- **disable** PF firewall
- **remove** PF rules, anchors, states, tables
- **uninstall** PF boot scripts

PF firewall will be disabled, no network filtering is applied any more. Boot scripts removed, PF will be disabled at system boot. If you manually enable PF then you will activate Apple-default configuration. IceFloor rules has been completely uninstalled.

Advanced options

Custom services

If you need to allow access to a service not listed in main IceFloor window then you have to manually add it as a custom service. Insert **service port numbers** in TCP and/or UDP text fields. If you need to add more than one service then separate port numbers with a **white space**.

If you know the service name but you don't know which port/ports it uses, click LIST. A new window will open with a **list of well-known services** with their own protocol and port number. Please note: some service needs more than a port. Please be sure to add the port to the correct protocol.

Black List

Black list is a list of IP addresses or subnets. All network traffic from/to this list is **blocked** by firewall rules installed by IceFloor. Use this list to block access to your mac from untrusted computers on your network, or to block outgoing traffic. For example you may want to block traffic from applications.
Insert as many addresses as you need, separate them with a white space.
You can also **import address list from text file**. The IceFloor parser will try to find IP addresses inside the imported file, so there is no need to use a specific format. The file must be plain text.

White List

White list is a list of IP addresses and subnets. If you select action "**Allow only a list of IP addresses (White List)**" in main IceFloor window, then selected services will be accessible only by hosts included in White List. If you leave the White List empty then all accesses to selected services will be blocked.

Advanced filtering

Black list and White list are global list. They affect all selected services.
If you need a more granular approach to filtering then you have to choose the IceFloor "Advanced filtering" feature.
If you need to allow access to **each service** by a **dedicated IP list**, then open the Advanced filtering window. Insert new records into the table using the text fields at the bottom.
For each new service you need to specify its protocol and choose a list of IP addresses or subnet allowed to connect.

Every time you make a change to Custom services, Lists or Advanced filtering, you have to click again "**Enable PF firewall and install boot scripts**" in main IceFloor window to update PF status. Please note: changes to PF configuration made outside IceFloor will be lost.

IceFloor reports: states and logs

PF states

PF states shows active states. States are created dyamically by PF when an allowed connection starts. Look at this window to see which connections are currently open and in which status.

Firewall Logs

IceFloor installs **boot scripts** in order to start PF firewall, load PF rules and **enable PF logging** every time you boot your mac.
The IceFloor ruleset **logs blocked packet by default**. Every attempt to connect to a blocked service will be logged to /var/log/pffirewall.log.
You can **read and search logs** in IceFloor clicking “Show firewall Logs”.

Real time logs

Click “Real time logs” to open a terminal window. You will see **logs in real time** while they are recorded. The shell command is “tail -f /var/log/pffirewall.log”.
Hit CTRL-C and CMD-W to close real time logs window.

Blocked hosts: list bad guys and block them

You really want to know who is trying to access your blocked services. Click “Blocked hosts statistics” to open a new window. Click “Show blocked hosts” to **parse log file** and show a list of the most **frequent IP addresses blocked by PF**.
Please note: depending on your rules, you may find a lot of records from local computers trying to “innocently” access your mac’s services.
If you find a suspect IP address and you want to block it then select it and click “**Add selected IP to blacklist**”. All traffic from/to this IP will be **blocked**. The IP address will be permanently added to the Black List. To delete it you must manually edit the Black List text field in IceFloor “Advanced options” window.
Please note: if a connection to this IP is already active you must **restart PF** in order for the connection to stop. Click “Enable PF firewall and install boot scripts” in main IceFloor window to restart PF.

Connections

List applications and network connections. Use this tool to find **unwanted outgoing traffic**.

IceFloor rules manager

Browse rules

Browse PF rules tree. Double click on anchor name to see it's contents, click "PARENT ANCHOR" to go back to parent anchor.
PF rules are structured in a tree almost like files. Rules containers are called **anchors**.
PF uses also **tables**. Tables are IP addresses container. Tables are relative to their anchor. Each anchor may contain its own tables.
IceFloor rulesets includes 2 anchors. Each anchor has their own default tables. Anchor 800.icefloor uses 2 tables: whitelist and blacklist. Anchor 800.icefloor/800.icefloor.advanced uses one table for each service added in "advanced filtering" table.

PF is different from IPFW. Rules activated by PF sometime have a different syntax from their respective configuration file. If you come from IPFW then you should read manpages for pf.conf and pfctl (man pfctl , man pf.conf).

The text field at the top of rules table represents current **PF logical path**. If empty it represents the main PF configuration file /etc/pf.conf, the PF logical path root.
You can edit the configuration file for current path (anchor) clicking "Edit current configuration file".
You can add a rule manually or use the **Rule Assistant**.
Use the Rule Assistant to add new rules and learn PF syntax. After reading PF manpages look at rulesets installed by IceFloor in /etc/pf.anchors .

Edit pf rules

Use buttons to **add** and **remove rules** and **anchors**, **tables**, reset firewall, modify firewall installation.
If you manually **edit a configuration file**, come back to IceFloor and click "**Reset and reload PF**" to see how changes affects network traffic. You can't edit IceFloor proprietary tables, just your own custom tables. Please use "Advanced options" to edit IceFloor tables (blacklist, whitelist, advanced*)
Use the **editor** to edit current anchor configuration file.

Import and export IceFloor configurations

Click menu bar "Files" and select "Import" or "Export".
IceFloor configuration are exported to and imported from a directory containing 2 files:
IceFloor.conf and IceFloor.adv.conf
After importing IceFloor configuration click "enable" in main IceFloor window to activate imported rules. Please note: you are NOT exporting PF configurations! you are exporting IceFloor configuration: services buttons status, action status, custom TCP/UDP ports, whitelist, blacklist and advanced filtering rules. All this stuff is contained in 2 conf files. Exporting or importing IceFloor configuration actually is importing/exporting a directory containing these two files.

IceFloor tips

Please note: click **“?” buttons** to see contextual helps. There are many of them.
Check also tooltips: hold mouse pointer on buttons or text fields to get some descriptive help.

If you want to use IceFloor rules manager/editor please remember, do not click “Enable PF firewall and install boot scripts” in main IceFloor window or your custom **PF configuration will be lost**. To enable/disable PF or boot scripts please use buttons in “Manage PF rules” window.

Every time you restart PF, **current active connections may be blocked**. This is normal as PF states are reset by IceFloor. Please be aware of that if you use IceFloor from a remote computer (screen sharing).

To completely **uninstall IceFloor** select Uninstall from menu bar.

Custom tables are persistent, they will be active also after a PF configuration reset, they must be deleted from “manage pf rules” window.

adding or deleting a new rule, a new anchor, a new table or a new IP in table will also reset PF and **reload PF configuration** from /etc/pf.conf

If you need to **disable logging** you can 1) edit pf configuration file to remove “log” option from rules or 2) disable logging in boot script (/etc/icefloor.sh)

Using IPFW and PF together is insane. You should avoid it. **PLEASE NOTE: when you enable IceFloor, all files installed by WaterRoof and NoobProof will be deleted including boot scripts** (plists and /etc/waterroof.sh). IPFW rules will be flushed and they will not load at boot. Please backup your IPFW configuration before using IceFloor.

“System services” service in service list should be enabled if you use **DHCP** on your network.

The PF **traffic shaping** (ALTQ) is not available in OS X. The XNU kernel lacks ALTQ support. We are stuck at dummynet, which is part of the deprecated IPFW firewall. Use **WaterRoof** to put selective **bandwidth** limit using dummynet on OS X Lion.

To learn PF open a terminal window and type:
man pf.conf
and later
man pfctl
then open www.openbsd.org and search for PF guide.

Good luck.

IceFloor

www.hanynet.com

developed by **Hany El Imam**

source code is available at **hanynet.com**

for information or **PayPal donations**:

hany@hanynet.com

Thank you.

Grazie.