

Murus 1.1

User Manual



Welcome to Murus

**Please read carefully this manual before using Murus.
In case you need support please visit our support site:**

www.murusfirewall.com/support

or contact us at:

info@murus.it

Enjoy!

The Murus Team

Introduction	6
<i>Welcome to Murus</i>	7
<i>OS X Firewalls</i>	7
<i>Murus is a front end</i>	8
<i>Murus installation is safe</i>	9
<i>Install Murus</i>	9
<i>Uninstall Murus</i>	9
<i>Murus flavors</i>	10
<i>Murus Comparison chart</i>	10
<i>Murus Logs Visualizer flavors</i>	11
<i>Murus Logs Visualizer Comparison chart</i>	11
Quick Start	12
<i>Welcome View</i>	13
<i>Start Murus using predefined presets</i>	13
<i>Start Murus using the Wizard</i>	14
<i>Murus Boot Scripts</i>	14
<i>How PF starts at boot</i>	15
<i>PF Status</i>	15
Services and Groups	17
<i>Services</i>	18
<i>Services Library</i>	18
<i>Groups</i>	19
<i>Groups Library</i>	19
<i>Custom Groups</i>	19
<i>Special services and groups</i>	20
<i>Cloning special services and groups</i>	21
Firewall Rules	22
<i>PF Filtering</i>	23

<i>Default Murus Filtering Policy</i>	23
<i>The PF “quick” keyword</i>	23
<i>Three Layers of abstraction</i>	24
<i>1) Managed Inbound and Outbound Services views</i>	24
<i>2) Expanded PF Configuration window</i>	26
<i>3) Runtime rules browser window</i>	28
<i>Real PF Configuration</i>	29
<i>Manually editing Murus PF ruleset from shell terminal</i>	29
<i>Inclusive and Exclusive rulesets</i>	30
<i>The ALL SERVICES meta service</i>	31
Advanced Filtering	32
<i>Inbound Service Options</i>	33
<i>Set for accounting</i>	33
<i>Log connections</i>	33
<i>Notify blocks and access in Logs Visualizer</i>	34
<i>Static filtering</i>	34
<i>Less restrictive flags policy</i>	34
<i>Port knocking hidden service</i>	35
<i>Brute force adaptive service</i>	35
<i>Forward service to NAT client</i>	36
<i>Outbound Service Options</i>	37
<i>Pass no-state inbound replies</i>	37
<i>Open Ports Management</i>	38
<i>Manual Ports Management</i>	39
<i>Automatic Ports Management</i>	39
<i>Emerging Threats Ban List</i>	39
<i>Murus Preferences</i>	40
<i>General Preferences</i>	41
<i>Ports Preferences</i>	42

<i>Advanced Preferences</i>	42
<i>Port Knocking Preferences</i>	43
<i>Logs Preferences</i>	44
<i>Proactivity Preferences</i>	44
PF States Inspector	45
<i>Understanding PF States</i>	46
<i>Keeping State for UDP</i>	46
<i>Murus uses PF stateful inspection</i>	46
<i>Murus PF States Inspector</i>	47
<i>State Inspector Info Popover</i>	47
<i>Blocking a connection</i>	48
<i>Kill PF States</i>	48
<i>Service Hosts Inspector</i>	49
NAT and Port Forwarding	50
<i>Share your Internet connection</i>	51
<i>Murus NAT</i>	51
<i>WAN and LAN network interfaces</i>	52
<i>NAT Groups</i>	53
<i>NAT Blocking policy</i>	54
Murus logic by examples	55
<i>Example 1: Dealing with PF States</i>	56
<i>Example 2: Rules Order</i>	58
<i>Example 3: Inbound per-service block rule option</i>	61
<i>Example 4: Logging and Notifications</i>	62

Please note:

This manual covers all Murus Pro features. Some feature is not available in Murus Lite and Murus Basic.

Section 1

Introduction

*Introducing Murus Pro and PF.
Information about OS X firewalls.*

Welcome to Murus

Murus is a front end for the OS X built-in PF network firewall.

It's main purpose is to speed up network firewall configuration and testing, using a simple interface. Filtering rules and networking options can be set dragging and dropping icons, changing their order, and selecting check boxes. There is no need to learn code syntax or to type shell commands. Everything is managed by visual elements like buttons, collections, lists, icons, leds.

OS X Firewalls

OS X is one of the most secure computer operating systems today. It features a solid UNIX base and a lot of security features. OS X from the very beginning shipped with a pre-installed firewall named IPFW. Directly derived from other less-known operating systems like *BSD, IPFW has been the default OS X firewall from Mac OS X 10.0 to Mac OS X 10.6. Apple started changing it's firewall policy with Mac OS X 10.5, introducing a built in application firewall, ALF, that can be configured from System Preferences Security preference pane, while IPFW can be configured only using the shell Terminal. On the other hand, Mac OS X Server featured a very simple IPFW graphic front end.

OS X 10.7 officially introduced a new network firewall, PF, and deprecated the old IPFW. Both PF and IPFW were installed but PF was the preferred choice according to OS X man pages, even if IPFW was the preferred choice for Mac OS X Server 10.7, according to Apple corporate web site.

IPFW survived until OS X 10.9, then it's been removed from OS X 10.10.

PF is a much more powerful and flexible network firewall. OS X PF implementation is derived from OpenBSD 4.3 PF, with some tweaks made by Apple. Most notably, traffic shaping is achieved using Dummynet, while ALTQ has totally been left out from OS X PF.

Currently OS X 10.10 Yosemite features two firewalls:

ALF: application level firewall, can be easily configured using System Preferences Security panel. It allows or blocks network connections at application level.

PF: network firewall, can be configured using the shell Terminal or using a third party front end, like Murus. It allows or blocks network connections at network level, letting you build and customize a complex network infrastructure.

Both firewalls are disabled by default on a newly installed OS X system.

While ALF is quite easy to enable, and does not require a real configuration, PF does require a deep knowledge of its syntax and logic, and requires the user to manually edit configuration files. PF firewall and PF network monitoring has to be done from the command line. The average user really needs a graphic front end for PF in order to manage firewall rulesets.

Both PF and ALF firewalls can be activated simultaneously, and they will work together. Their approach to network filtering is different, and they follow different logic patterns.

The same is true for third party firewalls. Every application firewall can seamlessly work together with a network firewall. So, for example, the user can run PF network filtering using Murus and application filtering using LittleSnitch in place of ALF.

We suggest to turn off ALF and all other network- and application-firewalls when using Murus for the first times. It is easier to understand how Murus affects networking if PF is the only running firewall.

It is also mandatory to uninstall any third party PF front ends like IceFloor and PFLists before starting Murus. To correctly uninstall IceFloor and PFLists please use their in-app specific buttons, do not try to uninstall them manually.

Murus is a front end

Murus is NOT a firewall. Murus a graphic interface (“front end”) for PF. Actually, Murus is much more, because it does a lot more than simple filtering. It lets the user create complex sets of rules, with advanced options like port knocking, adaptivity, accounting, notifications, and much more. The user can monitor network activity, services activity, logs activity in realtime and can interact with connections and rules.

PF ruleset can be managed at **three different levels of abstraction**:

- the intuitive collection of icons representing services and groups;
- expanded PF ruleset with each rule coming with descriptive icons, and a detailed dynamically created comment;
- true-realtime PF browser with anchor-path browsing and pf-table listing.

The user is able to configure and debug the PF ruleset combining these three levels of abstraction simultaneously. The ‘Test’ button is also available, and helps debugging the ruleset without modifying runtime rules. ‘Test’ is able to find errors in PF configuration, and displays the rule that generated this error.

Murus logic lets the user choose between inclusive and/or exclusive approach to filtering. And this is true at every Murus level: groups, services, logs, accounting,

NAT. Features like groups interface binding and custom policies let the user access a nearly infinite number of PF configurations.

All these features are be accessible by simply dragging and dropping icons.

Experienced system administrator will be able to add custom PF rules, and to manage mixed rulesets with both Murus generated rules and custom rules.

Murus installation is safe

Unlike many other Mac “firewalls”, Murus does not modify OS X PF default configuration and does not install any kernel extensions. It makes use of **tools and functions already built into OS X**, using its own configuration files. Here is some info:

PF is built into the OS X kernel

Murus PF configuration is saved in `/etc/murus/`

Murus PF boot scripts are stored in

`/Library/LaunchDaemons/it.murus.murusfirewallrules.plist` and `/etc/murus.sh`

Murus library is stored in `/Library/Preferences/it.murus.muruslibrary.plist`

Murus user preferences are stored in `~/Library/Preferences/it.murus.Murus.plist`

Murus adds an entry to both `/etc/syslog.conf` and `/etc/newsyslog.conf` in order to activate PF logging and log file rotation.

Murus uses the built-in `tcpdump` utility to manage PF logs

Being only a front end, **when your PF firewall is running you can quit the Murus application**. You don't have to keep it running because it's useless and potentially dangerous if you leave your keyboard alone. You should run Murus only for monitoring connections or for testing configurations. Once active, PF does not need Murus to be running and you can even trash Murus app. PF relies only on textual configuration files created by Murus.

Install Murus

Download ZIP file from www.murusfirewall.com, unzip it and open the DMG disk image. Copy Murus icon to your desktop or to your Applications directory, or wherever you want. Right click Murus icon and select “Open” to start Murus. If your system is set to open only applications from known developers then a dialog will appear, and you have to confirm in order to start Murus. Now you need to provide a valid administrator account. Then you have to type your activation email and serial number to activate and start Murus. You are now ready to setup and start your PF firewall.

Uninstall Murus

Reverting your OS X system to factory default is a very easy task. Select “Murus” menu and click “Uninstall Murus”. Restart your Mac. Your Mac is now cleaned and all files installed by Murus has been deleted. PF configuration has been restored to factory default and PF has been disabled.

Murus flavors

Murus **Lite**

Murus **Basic**

Murus **Pro**

Murus Comparison chart

	Murus Lite	Murus Basic	Murus Pro
Price	FREE	See murusfirewall.com	See murusfirewall.com
License	Commercial	Commercial	Commercial
Configuration Wizard	X	X	X
Ports management	X	X	X
Inbound filtering	X	X	X
Inbound logging	X	X	X
Expanded PF Config.	X	X	X
Predefined Presets	5	7	7
Outbound filtering		X	X
Outbound logging		X	X
Port knocking		X	X
Adaptive firewall		X	X
Advanced Filtering		X	X
Custom rules		X	X
Proactivity		X	X
Realtime PF Browser		X	X
Totally custom ruleset			X
Manual custom rules			X
Accounting			X
NAT and forwarding			X
Hosts Inspector			X
PF states Inspector			X
Murus Logs Visualizer	available separately	available separately	included

Murus Logs Visualizer flavors

Murus Logs Visualizer

Murus Logs Visualizer **Tryout**

Murus Logs Visualizer Comparison chart

	Murus Logs Visualizer Tryout	Murus Logs Visualizer
Price	FREE	See murusfirewall.com
License	Commercial	Commercial
Realtime ports monitor	limited to blocked inbound logs	X
Realtime addresses monitor	limited to blocked inbound logs	X
Realtime notifications	X	X
Simplified Log	limited to last 100 log lines	X
Manage Ignored ports/IPs		X
Graphical log statistics	limited to blocked inbound logs	X
Usage limits	app closes after 30 minutes	none

Section 2
Quick Start

Learn the basic

Welcome View

Main Murus window will start with a welcome screen displaying Murus version. Most Murus functions are available in the main window toolbar.

The two most important things in Murus are Services and Groups. You need to assign groups to services, and assign services to Inbound and/or Outbound areas in order to create a firewall ruleset. You have two main containers: the former for services and the latter for groups, both filled with some predefined content. You will be able to add new services and new groups.

Each Murus icon has a specific meaning and purpose. Please use Contextual Information panels to find tips and legenda. They are spread all over Murus interface. Click the blue “i” buttons to open these panels.

Configuring Murus Services and Groups requires you to understand Murus and PF logic. So you should read this manual before trying to do that.

However you can start Murus just right now, using Murus Wizard or Murus Presets. You will be able to further modify configurations created with both.

Start Murus using predefined presets



Move the slider to choose between different presets. The first preset is the most unsafe, the last is the most safe and restrictive. Click the button below to activate selected preset. Current Murus configuration will be overwritten by this new preset and PF will be started.

UNSAFE SAFE

4 **Almost all services blocked**

Almost all inbound services blocked except essential services like mDNS, NTP, Dynamic Ports range, which are open the LAN clients. Unlimited Internet access. Logging disabled. This is a safe preset and should be used when this Mac is connected to an untrusted network.

Activate selected Murus preset and start PF

Click the Presets button in Murus main window toolbar to open the Murus Presets popover view. Use the slider to display all available presets.

Click the blue button below to activate selected preset. Now PF is active using rules generated by Murus. You can modify current rules adding and removing services and groups or changing options. Remember to click “Start” in the toolbar every time you modify Murus configuration in order to update runtime PF rules and apply changes.

Start Murus using the Wizard

Click the Wizard button in the toolbar to start the Murus Wizard.

The Wizard is the most easy way to start using Murus. It will analyze the Mac to search for local listening (open) ports and display a list of corresponding Murus Services. Then you have to choose the access rules for these services.

The Wizard will also give the opportunity to set some basic options like logging, notifying and ban list protection. At the end of the procedure the PF firewall will be started and main Murus window will appear. Now it is possible to further modify the Murus configuration. Remember to click “Start” in the Murus toolbar to apply changes.

The Wizard enables by default the Unmanaged Ports Check. If you remove a managed service added by the wizard and the corresponding local port is still open (listening) then you will see an alert in the bottom left corner of the main Murus window.

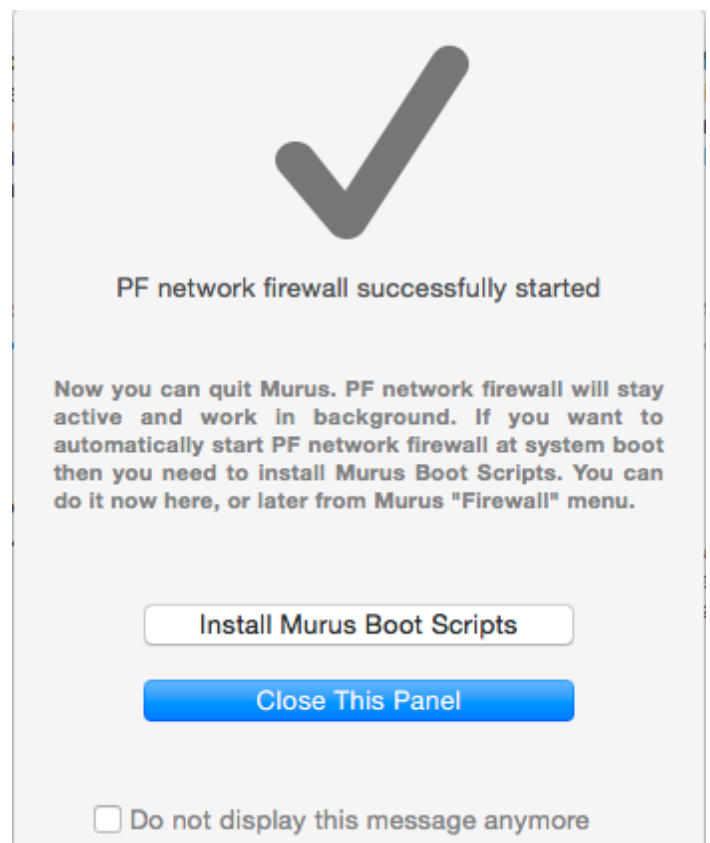
Murus Boot Scripts

If this is the first time you start Murus, a popover view will be displayed asking you if you want to install Murus Boot Scripts.

Boot Scripts allow your Mac to automatically activate PF firewall rules every time it starts. Scripts are also needed in order to enable the PF logging system.

This popover will appear every time you start (or restart) Murus until you install boot scripts. If this message is annoying, you can check the “Do not display this message anymore” check box before closing this popover in order to disable it.

You will be able to install and uninstall boot scripts at any time from Murus menu bar -> Firewall -> Boot Scripts.



How PF starts at boot

PF is loaded at boot time using two different files:

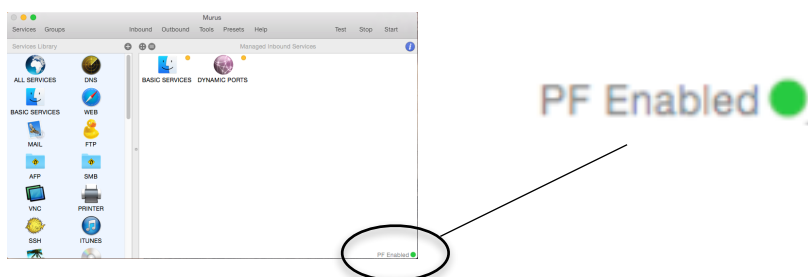
- 1) **it.murus.murusfirewallrules.plist**, stored in `/Library/LaunchDaemons`, is a launchd item. This thing is responsible for executing a bash script at system startup.
- 2) **/etc/murus.sh** is a bash script executed at startup time. Its purpose is to enable PF and to load PF rules generated by Murus. It also creates the “pflog0” network interface needed for PF logging, and starts the PF logging system using tcpdump.

Problems loading PF rules at system boot

PF will not load at boot if you configured PF using network interfaces that are not available at boot time, for example VLANs. To overcome this problem you should write your custom PF rules putting interface names in parenthesis, like `(vlan0)` or even `(vlan3:network)`. Murus 1.1 automatically manages this so you have to take care only of your custom rules.

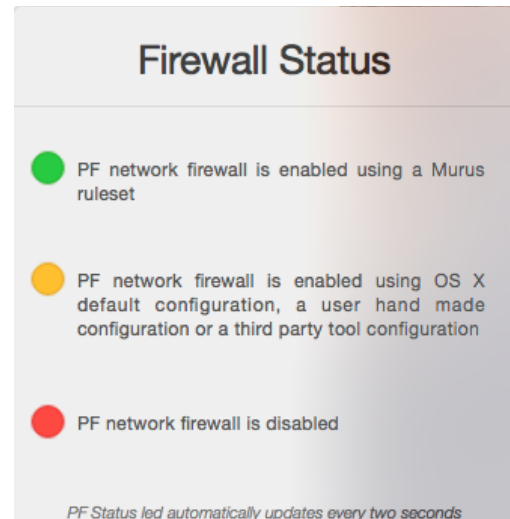
PF Status

If you never used PF on your Mac and you run Murus for the first time, PF will be probably disabled. PF status is displayed in the Murus main window's right bottom corner as shown in the screenshot below. If disabled, you will see a red led instead if a green led.



The led color and the text message indicate PF Status.

- **GREEN:** PF is active using a Murus ruleset.
Please note that this does not necessarily means that current Murus configuration and current PF running rules do match.
- **YELLOW:** PF is active but it is not using a typical Murus ruleset. So probably it is active using a custom ruleset or the default OS X ruleset.
- **RED:** PF is not active.



Please note that both the shell terminal `pfctl` command and Murus Runtime PF Rules Browser will display current runtime PF rules even if PF is disabled. You may also use the shell terminal to enable or disable PF:

ENABLE: `sudo pfctl -e`

DISABLE: `sudo pfctl -d`

To manually load Murus PF ruleset you have to enable PF and then load the ruleset with this shell command: `sudo pfctl -f /etc/murus/murus.conf`

Section 3

Services and Groups

Introducing Murus Services and Groups.

Learn how to manage Murus objects in order to build your own firewall ruleset.

Services

A Murus Service is an object with an icon, a name, a description, a ports list and a protocol (TCP, UDP, TCP•UDP, or TCP•UDP•ESP•GRE). This is used to represent network services, typically TCP and UDP services for which you run clients and or servers on your Mac.

Services Library

'Services' toolbar button opens/closes the Services Library view. Services Library is a collection of icons, each one representing a network service, for example FTP, SSH, PRINTER, MAIL. These are all services known to Murus. Select a service icon and click the magnifier button to open the service popover window and see descriptions, ports and protocol. Default services cannot be edited. You can, however, change their order in the library to meet your needs. To reorder services just drag and drop their icon.



Click the “+” button on right top of the Services Library view to add a new custom service. The service will be created at the end of Services Library. Select it and click the magnifier button to open the edit popover window. Change service name from “CUSTOM SERVICE” to a name that suites its purpose. Please do not exceed the available text space when choosing a new name. Define service port range by inserting port numbers separated by space. Define ports ranges using colon. Choose the service protocol: ‘all’ means ‘TCP and UDP’, while ‘esp/gre’ means ‘TCP,UDP,ESP,GRE altogether’. You may want also to write a short description for this service. You can have services using the same ports and even the same

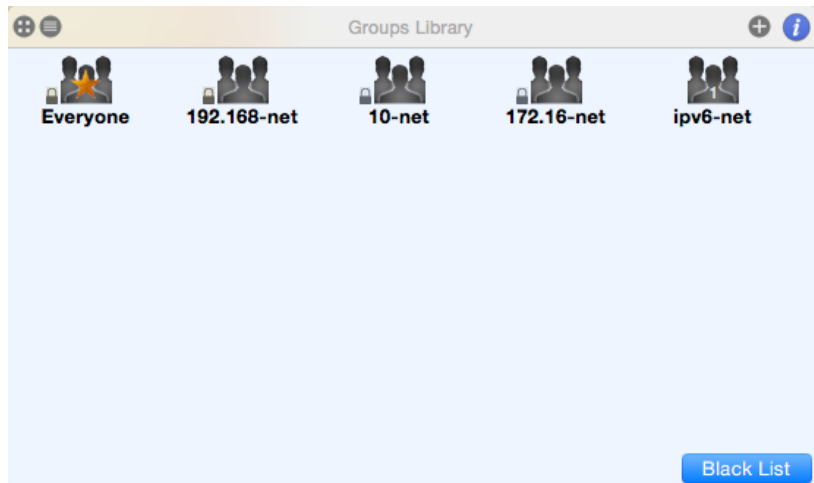
description, but not the same name. Services name is uppercase only, it may contain spaces and number but please avoid any special character.

Groups

A Murus Group is an object with an icon, a name, a network interface and a list of IP and/or Network addresses. They can be both ipv4 and ipv6 addresses. Network addresses must be in CIDR notation.

Groups Library

'Groups' button is located near the 'Services' button in the toolbar. Click it to open the Groups popover. Groups are represented by icons. Icons may appear differently according to the number of records and/or addresses contained in each group. A Murus Group holds a list of IP and/or network addresses and can optionally be bound to a network interface. Binding a group to an interface means that rules generated by this group will be effective only on such interface. Murus has 5 hardcoded groups that cannot be changed or modified.



Custom Groups

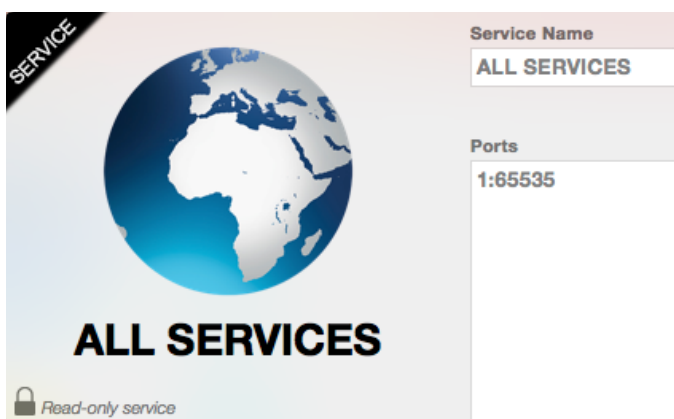
Click the “+” button to add custom groups. Choose a name for the group. Name must be lowercase and you should avoid using numbers, spaces and special characters. Use the popup button to bind the group to a specific network interface. If you don't want the group to be bound just leave 'all' in place. If you bind the group to a specific interface then all rules generated by Murus adding this group to a Service will be effective only on this interface.

Special services and groups

Murus makes use of some special services and groups in order to work properly. These special objects are already hardcoded into Murus and cannot be removed or edited. You will need to understand their meaning and their use in order to get the maximum freedom configuring your PF firewall.

Service **ALL SERVICES**

This meta-service represents all possible TCP and UDP services available, from port 1 to port 65535. This service is used to define to default policy for filtering, logging, and all other Murus services' options. This service can be put only at the beginning of your managed areas and cannot be moved.



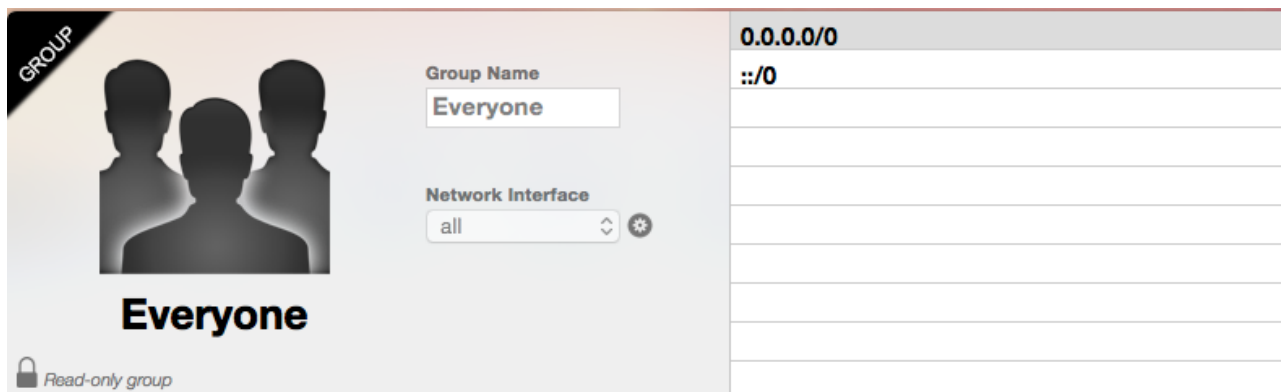
Service **DYNAMIC PORTS**

This service includes all TCP and UDP ports from port 49152 to port 65535. This range is known as “Dynamic ports” range. Many services (both clients and servers) may require connections on this port range, so it is a common practice to allow traffic on these ports. You can, however, decide to block this ports range. If you want to increase your security you can create a **custom service using the same ports range only for UDP protocol**.



Group *Everyone*

Groups *Everyone* represents the whole Internet. It contains two network addresses:



0.0.0.0/0 This means “All Internet ipv4 addresses”

::/0 This means “All Internet ipv6 addresses”

This group is used normally when you want to put general rules on services. It is bound to the meta-interface “all”, which means that it is effective on all network interfaces (except the lo0 loopback interface which is totally ignored by Murus PF ruleset).

Cloning special services and groups

In some cases you may need to create copies (clones) of “special” services and groups. For example you may need to create a copy of the ALL SERVICES service when you want to assign different rules to different network interfaces. And you also may need to create clones of “Everyone” group bound to specific interfaces. For example you create group “everyone_en1” bound to the en1 network interface.

Section 4

Firewall Rules

Learn how to display the PF firewall ruleset.

Introducing the three layers of abstraction used by Murus to manage PF ruleset.

PF Filtering

From OpenBSD PF manual:

Filter rules specify the criteria that a packet must match and the resulting action, either block or pass, that is taken when a match is found. Filter rules are evaluated in sequential order, first to last. Unless the packet matches a rule containing the quick keyword, the packet will be evaluated against *all* filter rules before the final action is taken. The last rule to match is the "winner" and will dictate what action to take on the packet.

Default Murus Filtering Policy

The recommended practice when setting up a firewall is to take a "default deny" approach. That is, to deny *everything* and then selectively allow certain traffic through the firewall. This approach is recommended because it errs on the side of caution and also makes writing a ruleset easier.

Traffic must be explicitly passed through the firewall or it will be dropped by the default deny policy. This is where packet criteria such as source/destination port, source/destination address, and protocol come into play. Whenever traffic is permitted to pass through the firewall the rule(s) should be written to be as restrictive as possible. This is to ensure that the intended traffic, and only the intended traffic, is permitted to pass.

The PF "quick" keyword

As indicated earlier, each packet is evaluated against the filter ruleset from top to bottom. By default, the packet is marked for passage, which can be changed by any rule, and could be changed back and forth several times before the end of the filter rules. **The last matching rule "wins"**. There is an exception to this: The quick option on a filtering rule has the effect of canceling any further rule processing and causes the specified action to be taken.

The PF quick keyword is used by some Murus hardcoded rules and can be optionally set for Murus custom rules.

Three Layers of abstraction

Murus lets the user configure firewall rules using three different layers of abstraction. Each one features its own logic and purpose.

- 1) **Managed Inbound and Outbound Services views:**
start configuration here
- 2) **Expanded PF Configuration window**
verify and understand configuration logic, add custom rules
- 3) **Runtime PF Rules Browser window**
see runtime rules to debug current running ruleset

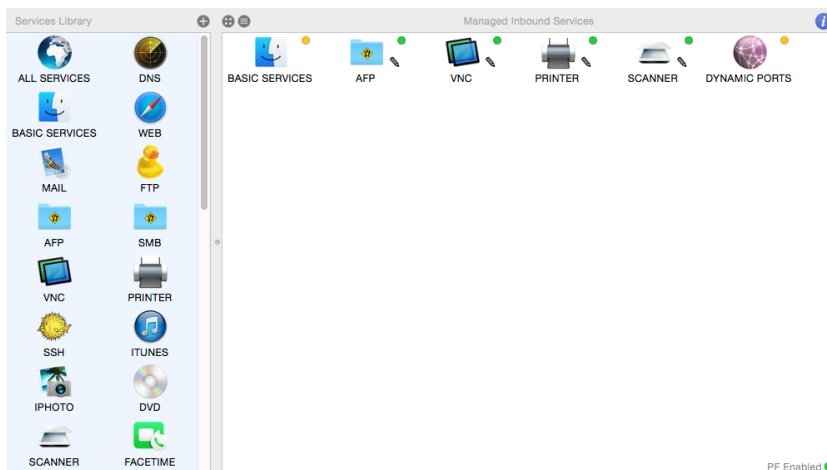
In addition, you may want to use **Murus Logs Visualizer**, to get a runtime simplified log file representation which allows you to fine tune both filtering and logging policies very easily. Murus Logs Visualizer is a standalone application available at www.murusfirewall.com.

1) Managed Inbound and Outbound Services views

These views represent the first layer of abstraction of your PF ruleset offered by Murus. Network filtering rules are generated assigning services to the “Inbound” and “Outbound” views, and assigning groups to such services. The “Inbound” view is the most important, because it’s the place where you decide how other people can access your Mac’s services from remote computers on the network.

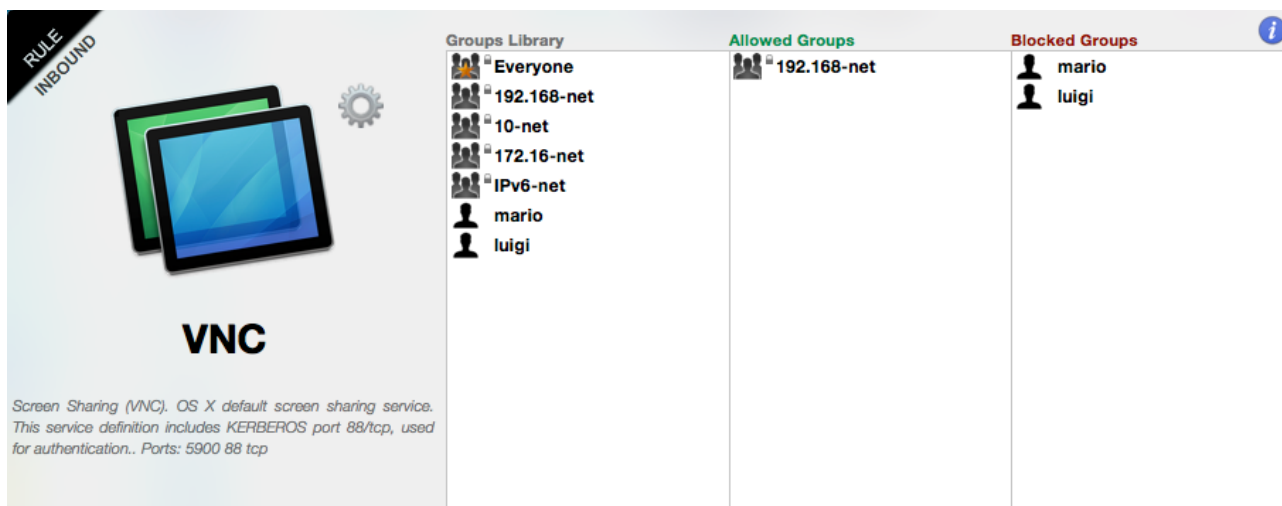
Select the “Inbound” view clicking the “Inbound” button, and drag services from the Services Library to the Inbound view.

By default, all services added have a green led. This means they access is allowed for everyone. You can change access rules for every service. Service led will change to yellow or red according to access rules.



Service Access Rules

Select a service in the “Inbound” view and click the magnifier icon to open the Service Rule Popover. Here you see 3 white columns. Drag groups from the column on the left (Group Library) to “Allowed Groups” and/or “Blocked Groups” in order to allow and block connections. Please note: block rules override pass rules. Blocks are meant to be used as exceptions to passes. For example you may put an entire C class in “Allowed groups” and put an IP belonging to this class in “Blocked groups”, as an exception.



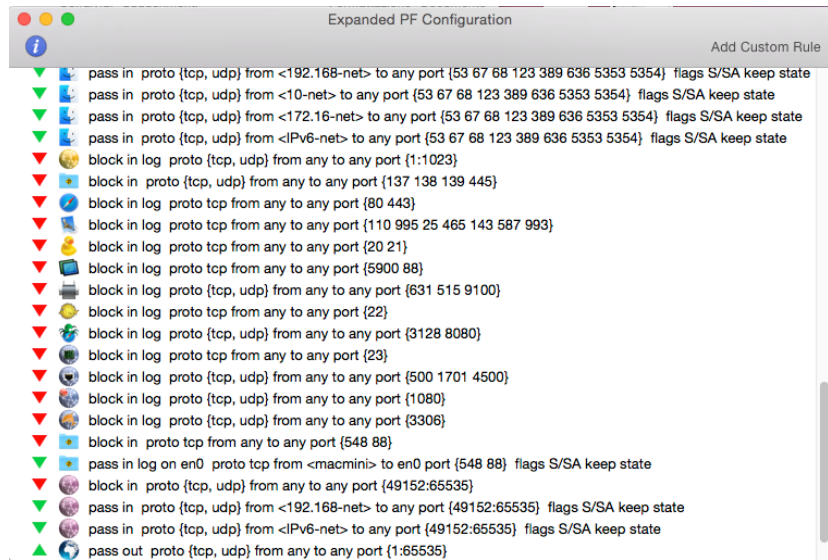
In this screenshot you see an example for the VNC Screen Sharing service. We assume groups “mario” and “luigi” contains their respective IP addresses in the 192.168-net class (for example 192.168.0.2 and 192.168.0.3). We assign the “192.168-net” group to “Allowed Groups” to allow connections to our local VNC service from all computers in the 192.168.0.0/16 network address space (from 192.168.0.0 to 192.168.255.255). Then we assign groups “mario” and “luigi” to “Blocked Groups” in order to override access permission for their IP addresses, blocking them.

Everytime you add a service to managed services and you assign groups to it, Murus generates new PF rules. In Murus Inbound and Outbound views PF **rules are generated reading services from left to right, row by row in both Inbound and Outbound areas**. To change rules order you have to change services icons order dragging and dropping services icons. Filtering Inbound connections is usually enough for a normal firewall configuration. If you feel paranoid you can also filter outbound connections. By default Murus allows all outbound configuration, leaving the ALL SERVICES alone with the green led in Managed Outbound Services view. This means that your Mac client applications are able to make all kinds of connections to remote servers. Filtering outbound is usually useful when you want to restrict the freedom of access to the network from your Mac. In case you run a NAT router with Murus please avoid applying unethical restrictions to your clients.

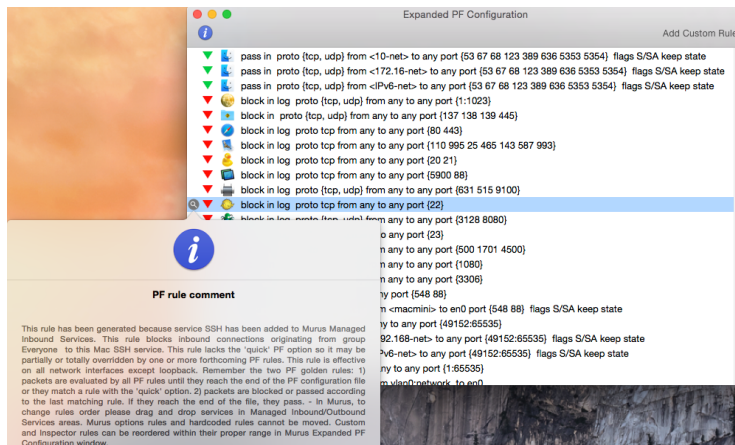
2) Expanded PF Configuration window

This window represents the second layer of abstraction of your PF ruleset. To open the Expanded PF Configuration window click the “Tools” button in the toolbar and then click the “Configuration” button. It is the second most important thing to understand in Murus.

In this window you see rules represented by icons and a string. Click the blue “i” button in the toolbar to see an explanation for all these icons and symbols.



Every time you add, remove or move a service or assign a group in Managed Inbound/Outbound Services views, the Expanded PF Configuration window is updated.



Rule Comment

Select a rule and click the magnifier button to display dynamically generated comment for this rule. This will help you understand why this rule is here, how to modify or remove it, and how it affects network connections. You can create your own comments for custom rules.

PF Rules and Anchors

PF rules are organized like files in a filesystem. Some rules are in the root, some others are in “anchors”. Anchors are rules containers just like directories are files

containers. Murus makes use of anchors to separate inbound and outbound rules from options rules.

Being a simplified layer of abstraction, **Expanded PF Ruleset does not show the ruleset as a tree but as an expanded view**. Rules are listed at the same level but rules order is preserved.

Please not that these rules does not necessarily represent currently active firewall rules. They represent instead the configuration obtained by current Murus configuration. Every time you make a change in Murus configuration, this window gets updated, but PF runtime rules are not. You have to click “Start” in Murus toolbar every time you need to apply changes.

Custom Rules

Click the top-right toolbar button to open the PF custom rule popover view. Here you can create a custom rule selecting values from popup menus and buttons, and typing addresses, ports and other optional rule parameters in text field.

You also have the option to create a manual pf rule, typing your own command. Click the “gear” button to open a new popover view to add a manual custom rule.

Filtering rules will be added to /murus.custom anchor. NAT rules will be added to /murus.nat anchor. Redirection rules will be added to /murus.rdr anchor.

To add a custom redirection rule you can select the “rdr” or “rdr pass” action, and use the specific form to set the forwarding IP address. Examples:

10.0.0.1 to forward to IP 10.0.0.1 using the same target port

10.0.0.1 port 45 to forward to 10.0.0.1 port 45

10.0.0.1 port {23 24 25} to forward to 10.0.0.1 ports 23, 24 and 25.

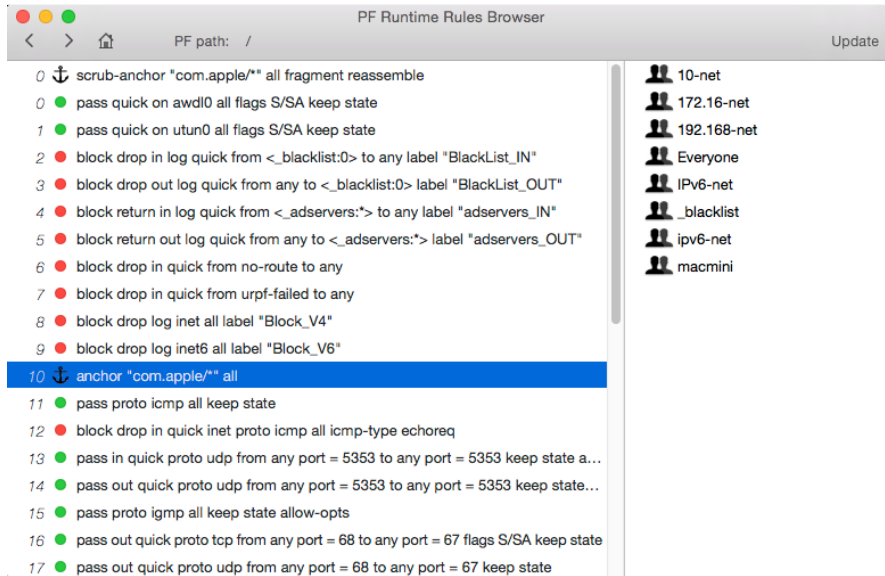
To add a custom NAT (translation) rule you need to add a manual rule clicking the gear button. You can add “nat on” or “nat pass on” rules. Please read the PF manual for more info about the syntax.

Custom rules can be edited. To edit a custom rule select it, click the magnifier icon to open the Info popover, then click the “Edit” button in its bottom right corner. The custom rules popover will appear. Make your changes and click the apply button. The rule is now changed. Click the “Start” button in Murus toolbar to apply changes to runtime PF rules.

3) Runtime rules browser window

This is the third layer of abstraction offered by Murus. It shows PF runtime rules in a browser-like window. These are true, live, running PF rules. This window automatically updates every time you click “Update” in Browser window or click “Start” in the Murus main window toolbar. This is the place where filtering actually

occurs and where you want to look when troubleshooting your ruleset. As you can see, **rules and anchor are numbered**. This is really important when reading log files, because each log line shows which PF rule has generated it. This is done by indicating the full rule path using rules numbers.



PF path

You see the current path on top of browser window. Starting path is the root, represented by “/”. Select an anchor and click the “>” or double-click it to change path and see its content. Click “<” button to go back one level, click the “home” icon button to go back to PF ruleset root.

PF tables

PF tables are used by PF to hold addresses list. Murus uses PF tables in order to simplify firewall configuration. Basically Murus creates a PF table for each Murus Groups defined in Murus Groups Library. There are also some hardcoded PF Table used by Murus rules engine.

Select a PF Table and click the magnifier icon to see the PF Table content.

Murus Groups are objects defined into the Murus application. PF Tables are runtime objects used by the OS X PF firewall.



While it is technically possible (and a common practice when creating manual PF configurations) to modify runtime PF Tables content, Murus does not allow to do it in its interface. PF Tables will be automatically created or modified every time you reload PF clicking the “Start” button in main Murus window, according to your Murus ruleset. You can, however, modify them using the `pfctl` shell command. This will obviously affect the PF ruleset in a way Murus cannot be aware of. So take care.

There is an exception. You can manually empty the “bruteforce” PF Table in “murus.inbound” anchor. This PF Table contains addresses blocked by the anti-bruteforce system provided by Murus. A “X” button will appear in the PF Table popover: click it to empty the PF table.

Real PF Configuration

The reason why we need 3 layers of abstraction is quite clear if you look at the real PF configuration file. It is stored in a hidden directory, accessible from the shell terminal or from the finder if you tweaked your system somehow.

The directory is `/etc/murus`.

It contains a bunch of files, most notably `murus.conf` which is the first file invoked by PF when reading its configuration. All other `murus.*` files are referenced in `murus.conf`. They contain Murus anchors’ PF rules and PF tables definitions.

Manually editing Murus PF ruleset from shell terminal

You should not edit manually Murus files stored in `/etc/murus`. If you do so, please remember that you have to restart PF from the shell terminal and not from Murus, or your settings will be lost (overridden by Murus). To start PF using a hand-modified murus ruleset you have to type this command in shell terminal:

```
sudo pfctl -f /etc/murus/murus.conf
```

You can’t use Murus to make changes (because you will loose your hand-made changes) but you can use Murus runtime browser to see active rules. **Instead of manually editing the ruleset**, you can select the Murus option to “**Disable Murus core ruleset**”. Select it in Murus Preferences, then open Expanded PF Configuration;: all hardcoded and dynamically generated rules are gone. You can add custom rules and create a totally customized PF ruleset using only your rules. Custom rules can be reordered and can be deleted from this window. You can add filtering, NAT and redirection custom rules and create a **totally functional and customized ruleset yet taking advantage of other Murus features**.

Inclusive and Exclusive rulesets

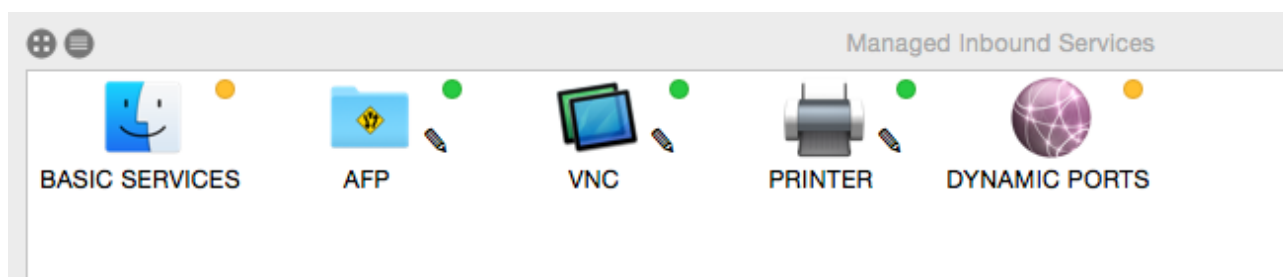
There are two basic ways to create firewall rulesets: “inclusive” or “exclusive”. An exclusive firewall allows all traffic through except for the traffic matching the ruleset. An inclusive firewall does the reverse. It only allows traffic matching the rules through and blocks everything else.

PF typically uses an inclusive approach to rules. In its starting configuration, Murus blocks all inbound connections except connections to “BASIC SERVICES” (mDNS, ldap, nntp, dhcp) and allows all outbound connections.

The meta-service “ALL SERVICES” holds all tcp and udp network services (from port 1 to port 65535). The meta-groups “Everyone” holds all IPv4 and IPv6 addresses. You should make use of them when dealing with inclusive/exclusive rulesets.

A way to increase granularity and to fine tune your firewall rules is to bind groups to interfaces. Assigning a group to a service Murus generates a PF rule. If such group is bound to a network interface, such rule will be effective only in that interface.

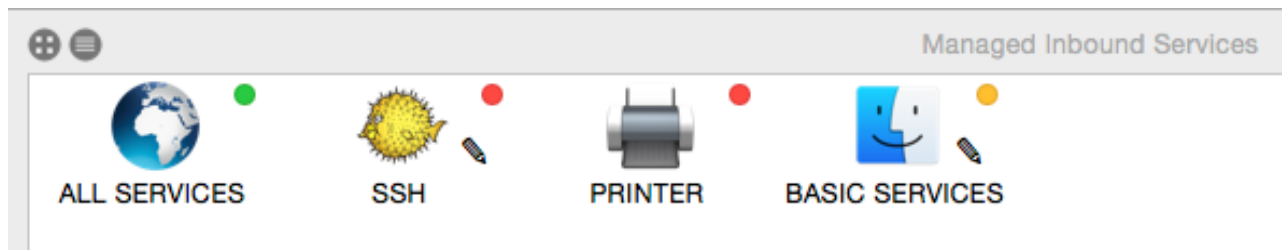
Inclusive Ruleset



Example of inclusive ruleset. All inbound connections are blocked, except connections explicitly allowed. In this screenshot we allow all inbound connections coming from everyone on the Internet and targeting this Mac’s local AFP, VNC and PRINTER services. We also allow inbound connections to BASIC SERVICES and DYNAMIC PORTS services, but with a restricted access underlined by the yellow led.

Please notice that this configuration lacks the ALL SERVICES service. There is no difference between adding the ALL SERVICES service with the RED dot, or removing the service. In both cases all services are blocked by default.

Exclusive Ruleset



Example of exclusive ruleset. Please notice the presence of ALL SERVICES special service with a GREEN dot. All inbound connections are allowed, except connections explicitly blocked. In this screenshot we allow all inbound connections from remote clients to local services, except connections to local SSH and PRINTER services. Like the previous example, service BASIC SERVICE has a yellow dot, meaning its access is restricted to one or more groups.

The ALL SERVICES meta service

Assigning the black or green pencil (or any other service option) to the ALL SERVICES special service affects the global policy. Rules are generated reading icons from left to right, row by row. All filtering rules and logging rules generated by adding icons to Inbound and Outbound views may be overridden by forthcoming rules. This is the reason why service ALL SERVICES can't be moved. If added, it will be put at the beginning of the icon list, because global rules generated by this service must be overridden by rules generated adding common services.

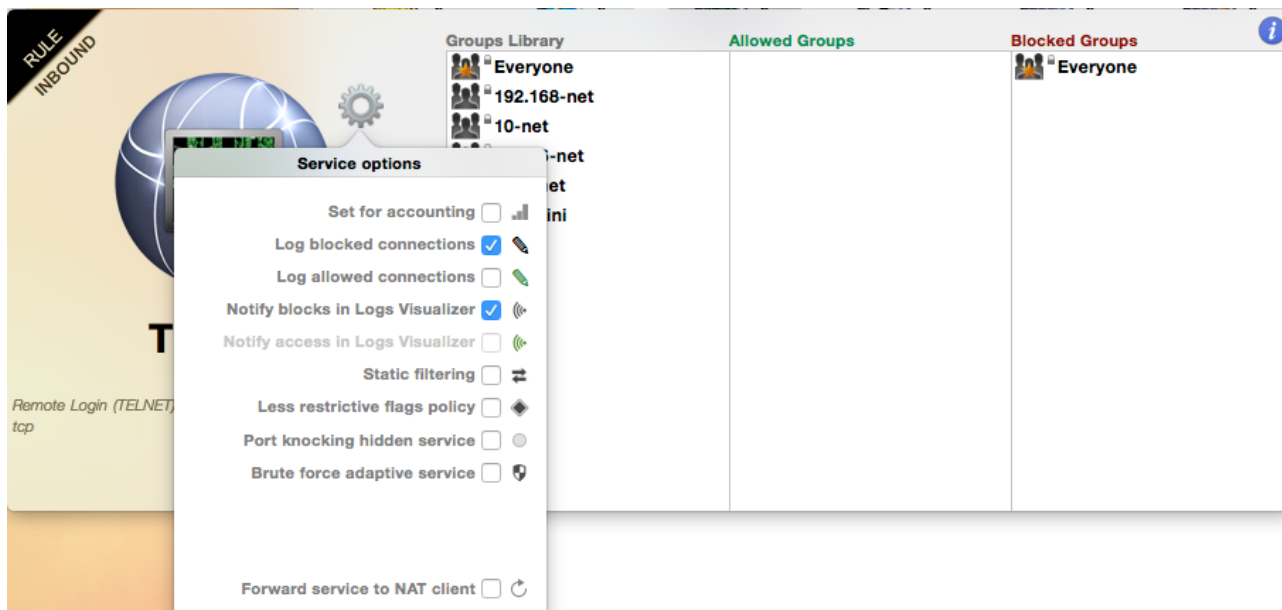
Section 5

Advanced Filtering

*Learn how to apply advanced services filtering rules.
Introducing port knocking, adaptive firewall and other options.*

Inbound Service Options

Select a service in Managed Inbound Services view and click the magnifier icon to open the Inbound Rule popover view.



Click the ‘gear’ button to open the “Service Options” popover view. This is the place where you configure inbound filtering advanced options.

Set for accounting

Set for accounting [bar chart icon]

Check this button to activate traffic counters for selected service. Access counters from Murus main window toolbar clicking “Tools” button and then clicking “Accounting” button. Counters will be reset every time you click “Start” in main Murus window toolbar.

Log connections

Log blocked connections [pencil icon]

Log allowed connections [pencil icon]

Check these buttons to explicitly log connections from allowed and/or blocked groups. Please note that these options are affected by global Murus logging policy and by Murus Advanced Preferences. More about this topic later in this manual.

Notify blocks and access in Logs Visualizer

Notify blocks in Logs Visualizer 

Notify access in Logs Visualizer 

Check these buttons to activate the Murus Logs Visualizer notification system for this service. Notifications will appear in the right top corner of your OS X desktop, together with all

other notifications from OS X apps, third party apps and web sites. Please note that this feature requires you to install and run Murus Logs Visualizer, which is a standalone application available separately from Murus.

These options are available only if logging is enabled for selected service.

Static filtering

Static filtering 

Murus uses stateful packet filtering by default for every service added to Inbound and Managed Outbound Services.

Static filtering is a particular way to allow connections to services. This option affects only “pass” rules, not “block” rules generated by this inbound service. Check this button to enable static filtering for this service. Access to service is granted by two rules: an inbound pass rule and an outbound pass rule. Stateful firewall is disabled for this service, so no states will be created for passed connections. All packets will be evaluated by the PF ruleset instead of flowing through dynamically created states. This option may be useful for services like KERBEROS or for some game.

Less restrictive flags policy

Less restrictive flags policy 

By default stateful packet filtering rules accept TCP packets only with S/SA flags. This is the most common practice with PF, but you may want to be more permissive

enabling access to packets with any type of flags. Check this button to enable this more permissive flags policy on selected service. This option may be useful in some case with services like AFP, SMB, NFS, WebDAV and such.

Please note that ‘Static filtering’ and ‘Less restrictive’ flags policy options are mutually exclusive.

Port knocking hidden service

Port knocking hidden service ●

Check this box to hide this network service using port knocking. Once selected, you will not be able to assign groups to this service. When set as hidden, a service will have the

“Everyone” group assigned to “Allowed Groups”. Its main led will turn grey.

Service will not be visible on the network. Its ports will show as “filtered” by network port scanners. Remote clients will not be able to connect to your service.

To connect to your service, remote clients must send a specific TCP SYN sequence to a specific list of ports, in a specific order. You define your own port knocking sequence in Murus Preferences window, in “Port Knocking” tab.

When a correct sequence is received by your Mac, PF will enable access to your local service for that specific remote client’s IP address. This remote client will be able to access your hidden service.

If a remote clients attempts to access your hidden service providing an incomplete or wrong knocking sequence, its IP address will be banned and considered hostile by Murus. All connections from this address will be blocked. To unblock an address you must access the port knocking management.

Port knocking authorizations are managed by the Murus Proactivity system. Click the “Tools” button in Murus main window toolbar, then click “Proactivity” button to open the Proactivity window. Click “Port Knocking” button in Proactivity window toolbar to manage port knocking authorizations and blocks. Here you can remove both authorizations and blocks selecting an IP address and clicking the “X” button.

Port knocking authorizations and blocks can be set to automatically expire at a given time. Open Murus Preferences, select Proactivity tab and check the option. Move the slider to choose the expire time. Click the save button to immediately activate the system.

Brute force adaptive service

Brute force adaptive service ●

Max. connections 4



Max. time (s) 33



Adaptive firewall is a way to proactively pass or block connections according to network activity quality, quantity, type, timings, and such.

Murus uses adaptive rules to block a very

common remote attack named “brute force”.

“Brute force” is a way to gain access to a network service trying login/password combinations from common lists or randomly generated lists. This is a way to get

unauthorized access to services like SSH and TELNET and others, and it is a potentially dangerous threat for everyone running such services.

Check this button to enable adaptive filtering for selected service. Use the sliders to set the max amount of connections (for each remote IP address) in a specific amount of time.

If a remote client exceeds these limits, PF will put its IP address in a specific ban list, and will consider it as hostile. All network connections from this IP address will be blocked.

Please note that some more sophisticated services may be able to offer the same protection at application level. Some other services (like AFP and VNC and other Kerberos based services) may suffer from such kind of adaptive filtering, so they require a specific care. In both cases you are advised to frequently monitor these services in case you set the adaptive option, and increase the value of both sliders in case you see IP addresses unexpectedly blocked.

Brute force blocks can be set to automatically expire at a given time. Open Murus Preferences, select Proactivity tab and check the option. Move the slider to choose the expire time. Click the save button to immediately activate the system.

Forward service to NAT client

Forward service to NAT client 

10.0.0.2

Optional port or range

Check this box to forward inbound connections to a NAT client. **This option is effective when you are using your Mac as a dual-homed router running Murus NAT**, and you want to make some of their

services available to the public. The easiest way to export a service is to check this box and enter the LAN IP address of your local NAT client. You can leave the ‘Ports’ field empty, so all service ports will be forwarded to the NAT client’s same exact ports.

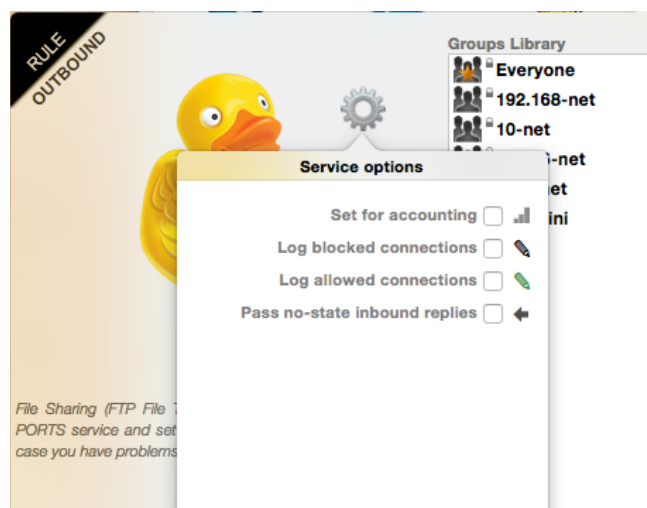
If you want to forward a service to different ports then you can specify them in the ‘Ports’ field but you have to take care because you must insert the same number of ports. For example if the service uses a range like “200 201 210:215” (that is a range made of 8 ports) you need to forward it to 8 ports, no more no less.

Please note that port forwarding will not work with OS X Internet Sharing. You need to do NAT using Murus. Please disable OS X Internet Sharing in OS X System Preferences -> Sharing prepane before activating Murus NAT.

Outbound Service Options

Select a service in Managed Outbound Services view and click the magnifier icon to open the Outbound Rule popover view.

The first three options has been covered in the previous chapter. Their effect on PF ruleset is the same. Obviously they will be applied to outbound rules.



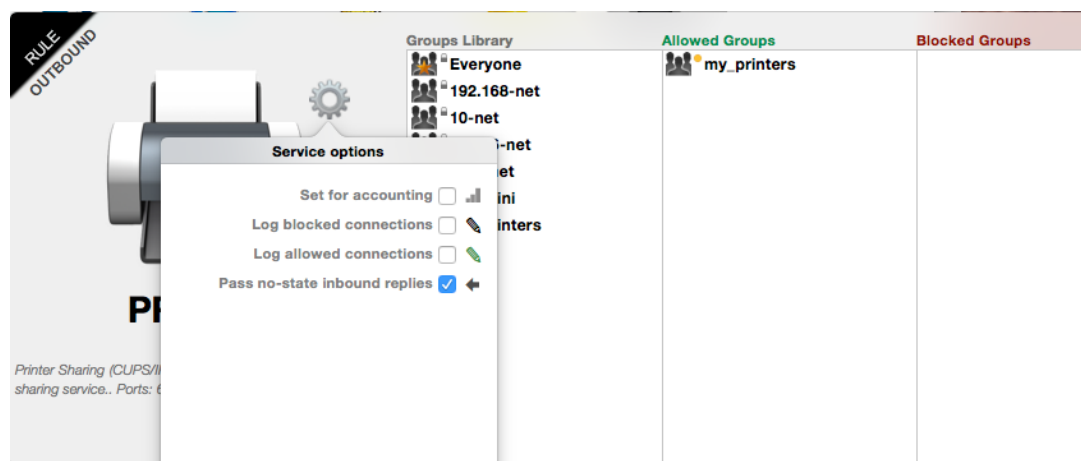
Pass no-state inbound replies

Pass no-state inbound replies ←

The forth option is an outbound-specific option used for services that require a “job monitoring” connection. **This option is important for PRINTER and SCANNER**

services. If you want to use a network printer and allow remote job monitoring (that is a very common feature for almost all OS X printer drivers or application bundles) you should add the PRINTER service to your Managed Outbound Service view and check this option. You should do this even if you are not doing any outbound filtering (you have only the ALL SERVICES service added with a green led). This option adds a static filtering rule to allow inbound traffic coming from remote service port.

For security reasons, the best practice is to activate this option only for services with a very restricted access. So, for example, you should assign to outbound PRINTER service only one group in “Allowed Groups”, and this groups should contains only your printers IP addresses.



Open Ports Management

Murus Ports Management is a tool used to help configuring the Murus Managed Inbound Services. The system works and is effective only when Murus application is running.

Open Murus Preferences and select “Ports” tab to open the Ports Management preferences. Select “Check local ports” to activate the system. Now Murus will continuously check for local listening ports.

If an open port has a corresponding service in the Murus Managed Inbound Services then it will be considered as “managed”. If an open port lacks the corresponding service in the Murus Managed Inbound Services then it is considered “unmanaged”.

Being “unmanaged”, connections to this port will be passed or blocked according to the global Murus inbound filtering rules. Managing a port means that you can assign specific filtering and logging options to inbound connections to this port. To manage a port you need to assign the corresponding service to the Murus Managed Inbound Services area.

This can be done in two ways: manually or automatically. By default Murus is set to handle this thing manually.

Manual Ports Management

If there are unmanaged open ports Murus will display an alert with a yellow dot in the left bottom corner in main window. Click this alert to open the Unmanaged Ports popover view, which displays all unmanaged ports and the corresponding Murus Service. Some time more ports can be nested in the same service. Some time Murus Service Library does not contain a corresponding service for a given port. In this case you will see a service with a generic icon and a generic name.

Select a service in the Unmanaged Ports popover and click the “+” button to manage the service. The service icon will disappear from the Unmanaged Ports view, and will appear in the Murus Managed Inbound Services area. It will be blocked by default. Select it to change access permissions. Runtime PF rules has not been changed yet: remember, you have to click “Start” in the toolbar to apply changes. Now the service is managed. You can proceed and click “+” on all unmanaged ports icons. The yellow dot alert will disappear when there are no unmanaged open ports.

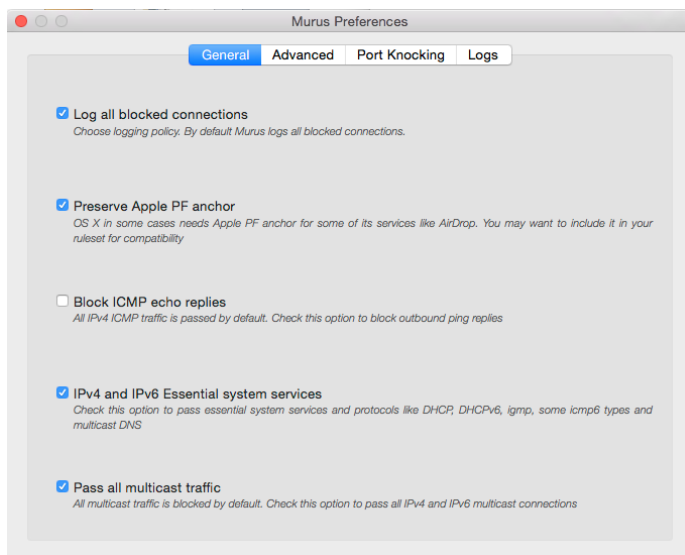
Automatic Ports Management

Select the “Auto Manage Ports” button to activate the automatic ports management. If an unmanaged open ports is detected then Murus will automatically assign the corresponding Murus service to the Murus Managed Inbound Services area. It will add it using permissions set in the Ports Preferences. You have 5 permissions options to choose from. The check is continuous but will work only if Murus application is open. Please note: this is not to be used as a “live” protection system. Automatic ports management should be used to help configuring the firewall, testing different scenarios and dealing with unknown/unpredictable app behaviors. It is a tool that works only when Murus app is running and is useful only for configuration, testing and debug. Murus application should normally be left closed because PF works in background.

Emerging Threats Ban List

Open Murus Preferences and select the Proactivity tab. Check the “Activate URL-based ban list protection and auto update” option to activate this protection system. OS X will silently download from a given URL a list of dangerous well-known IP addresses and block all inbound and outbound traffic from/to these IP addresses. This system works in background. Murus provides a default URL (from the free emergingthreats.net online service) but you can use your own URL. Use the slider to set the update frequency. If you use the default URL please set the slider to the maximum value (24 hours) for always-on Macs, and set it to 720 minutes (12 hours) for all other Macs.

Murus Preferences



Click the 'Murus' button in Murus menu bar then click the 'Preferences' button to open the Murus Preferences window. It is divided into four main sections. Use the tab buttons to switch between sections.

This is the place where you set some important options that affect PF filtering and logging.

1) General

Here we set some filtering and logging option.

2) Advanced

Here we set some very important options that affect the whole Murus filtering logic.

3) Port Knocking

This is the place where you configure access to hidden services.

4) Logs

Here we set PF log file rotation parameters.

General Preferences

There are five options in this section.

1) Log all blocked connections

By default this option is checked. This means that all inbound blocked connections will be logged to file. If you uncheck it then blocked connections will not be logged, except for services where the logging option is explicitly specified.

In case this option is checked and active, in order to avoid logging a blocked connection to a specific service from a specific group, you must add this service to the Managed Inbound Services view, assign the group to 'Blocked Groups', remove all groups from 'Allowed Groups' and verify that the "log blocked connections" option in Service Options is unchecked. This is a way to override the global block rule (which logs everything) with a specific per-service rule which blocks everything but does not log block to file.

2) Preserve Apple PF anchor

Some OS X service needs specific PF rules. These rules are included in a configuration file installed by OS X that contains Apple specific PF rules. You may decide to include these rules into your ruleset to maximize compatibility with some current or future OS X service.

3) Block ICMP echo replies

ICMP traffic is passed by Murus. You may want to block ICMP echo replies. This is useful if you prevent remote clients to be able to "ping" your Mac and obtain a reply.

4) IPv4 and IPv6 essential system services

Check this box to allow connections to some commonly needed network service and protocols, including DHCP, multicast DNS, IPv6 ICMP and IGMP. This option is useful to improve your experience while browsing the local network for services like file sharing or screen sharing. They are useful also for some OSX/iOS synch and pairing network activity.

5) Pass all multicast traffic

Check this box to allow multicast traffic. While this may not be necessary, it is a common practice to allow these connections. Uncheck it only if you need a

paranoid level of protection or if you have a strong valid reason to block multicast traffic.

Ports Preferences

Use this panel to configure the Murus Ports Management system, described in another chapter of this manual

Advanced Preferences

There are there groups of options in this section.

Inbound and Outbound per-service block rules

These two options are checked by default. They affect the way Murus generates rules when adding a Service to, in turn, Inbound or Managed Outbound Services.

When this option is unchecked and inactive, Murus will add for each managed Service:

- a pass rule for every group added to “Allowed Groups”
- a block rule for every group added to “Blocked Groups”

These rules typically override the global hardcoded block rules. The Murus (typically) inclusive approach to filtering relies only on the global blocking rules.

When this option is checked and active, Murus will add for each managed Service:

- a leading dedicated per-service global block rule that blocks all connections to this service
- a pass rule for every group added to “Allowed Groups”
- a block rule for every group added to “Blocked Groups”

The Murus inclusive approach to filtering now relies on both global blocking rules and on per-service blocking rule. This allows for a more granular approach to filtering and logging, but it's a tradeoff because it generates a bigger ruleset which may be more crowded and hard to understand.

Please keep the Murus Expanded PF Configuration window open in order to see how these options affect inbound and outbound filtering.

Enable normalization

Normalization is a common practice in most firewall setups. It is used to optimize the firewall filtering engine reassembling fragmented packets and discarding packets with invalid flags. This option increases firewall CPU usage and, in some case, may increase network latency affecting realtime applications.

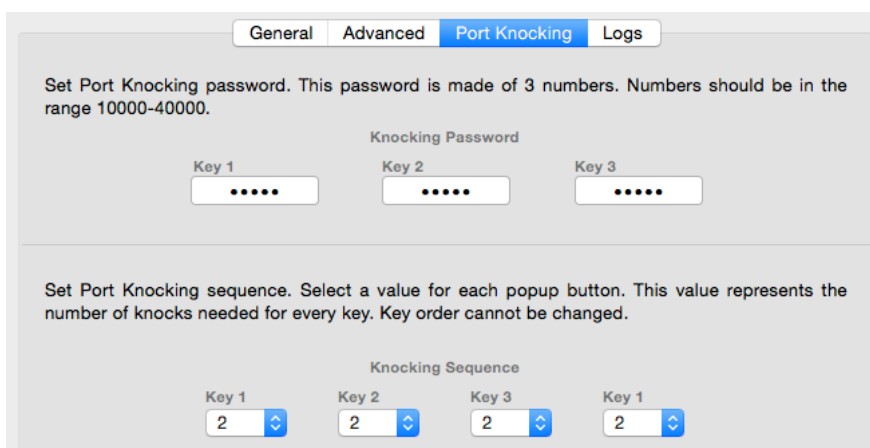
Disable Murus Pro core ruleset

Check this option to disable all Murus dynamically generated rules. This is useful if you want to configure a completely custom PF ruleset, starting from an almost empty ruleset, adding your own custom filtering, nat and rdr rules.

Port Knocking Preferences

This is the place where you define the sequence used to access your hidden services. You will share this sequence with your clients, in order to allow them to access your hidden network services.

First of all you need to define your knocking password, which is made by three numbers. Choose three random numbers in the range from 10000 to 40000. Type these numbers in text fields 'Key1', 'Key2' and 'Key3'. You will not be able to see typed number because they are hidden.



General Advanced **Port Knocking** Logs

Set Port Knocking password. This password is made of 3 numbers. Numbers should be in the range 10000-40000.

Knocking Password

Key 1 Key 2 Key 3

Set Port Knocking sequence. Select a value for each popup button. This value represents the number of knocks needed for every key. Key order cannot be changed.

Knocking Sequence

Key 1 Key 2 Key 3 Key 1

2 2 2 2

Then you have to define your knocking sequence. This is achieved selecting random numbers from the four popup buttons. Each button can be set with a value from 2 to 9.

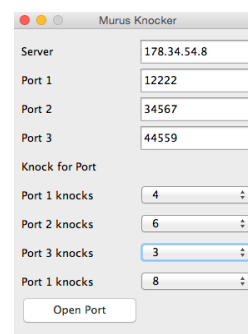
Remote clients needs to use the free and multiplatform Murus Knocker to get access to your hidden service. To be able to connect to your Mac's hidden services you must provide to your clients:

- 1) the knocking password made of 3 numbers
- 2) the knocking sequence made of 4 numbers
- 3) your public IP address

Clients providing the correct knocking sequence will have access to all your hidden services. Clients failing to provide the sequence will be blocked. Use Murus Proactivity to manage port knocking authorizations and bans.

Murus Knocker is free and available at www.murusfirewall.com. It requires Java. It has been tested on OS X, Linux, Windows.

Murus uses a specific PF anchor for port knocking rules. This anchor is generated only if you have at least one inbound hidden service.



Murus Knocker

Server 178.34.54.8

Port 1 12222

Port 2 34567

Port 3 44559

Knock for Port

Port 1 knocks 4

Port 2 knocks 6

Port 3 knocks 3

Port 1 knocks 8

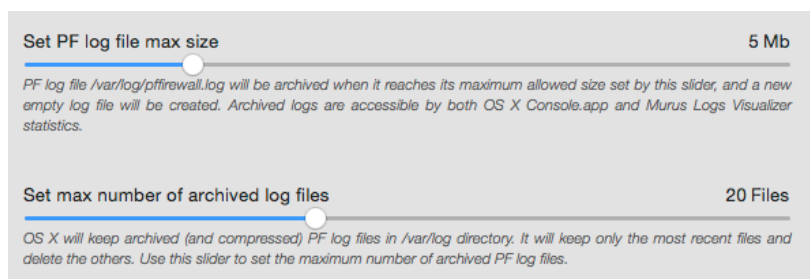
Open Port

Logs Preferences

Here you set only **log file rotation parameters**.

PF log file is stored in file `pf firewall.log` in `/var/log` directory. This file may become very big over time. When this file reaches a specific size, OS X archives it in a compressed file and generates a new empty log file. This procedure is named log rotation.

Archived log files are incrementally stored in `/var/log` directory and they can be directly accessed (without uncompressing them) by both OS X Console.app (found in your Applications/Utility directory) and Murus Logs Visualizer graphical statistics.



The first slider is used to define the maximum log file size, expressed in MBytes.

Once reached this size the file is rotated. Please note that this number refers to the size of the

plain uncompressed log file. When archived, log files will be much smaller.

In order to avoid filling your hard disk with log file (this may happen maliciously or not) you will have a maximum number of rotated log files. The second slider sets this limit. So if you set it to 15, OS X will keep only the latest (newest) 15 archived log files. So when you already have 15 archived log files, OS X will delete the latest (oldest) archived file when creating a new one. The number of archived log file will never exceed the number of 15.

Click the button to save log file rotation settings.

Log rotation preferences are stored in two default OS X system files in `/etc` directory:

- **syslog.conf**
- **newsyslog.conf**

These files are read by OS X at boot time. For this reason you must reboot your Mac to apply changes to the log file rotation policy.

Proactivity Preferences

Use this panel to automatically reset port knocking and brute force authorizations and blocks at a given time, and to optionally activate the Ban List protection system.

Section 6

PF States Inspector

Introducing PF states: learn how PF manages established connections using stateful inspection. Learn how to list and block active PF states using Murus.

Understanding PF States

From OpenBSD PF manual:

One of Packet Filter's important abilities is "keeping state" or "stateful inspection". Stateful inspection refers to PF's ability to track the state, or progress, of a network connection. By storing information about each connection in a state table, PF is able to quickly determine if a packet passing through the firewall belongs to an already established connection. If it does, it is passed through the firewall without going through ruleset evaluation.

Keeping state has many advantages including simpler rulesets and better packet filtering performance. PF is able to match packets moving in *either* direction to state table entries meaning that filter rules which pass returning traffic don't need to be written. And, since packets matching stateful connections don't go through ruleset evaluation, the time PF spends processing those packets can be greatly lessened.

When a rule creates state, the first packet matching the rule creates a "state" between the sender and receiver. Now, not only do packets going from the sender to receiver match the state entry and bypass ruleset evaluation, but so do the reply packets from receiver to sender.

All *pass* rules automatically create a state entry when a packet matches the rule. This can be explicitly disabled by using the Murus "Static filtering" option for Managed Inbound Services (which in turn generates a PF rule with the "no state" option).

Keeping State for UDP

UDP is a stateless protocol. While it is true that a UDP communication session does not have any concept of state (an explicit start and stop of communications), this does not have any impact on PF's ability to create state for a UDP session. In the case of protocols without "start" and "end" packets, PF simply keeps track of how long it has been since a matching packet has gone through. If the timeout is reached, the state is cleared.

Murus uses PF stateful inspection

By default all *pass* rules generated by Murus Managed Services and by Murus hardcoded/optional rule do use PF stateful inspection. A state will be created for each passed connection. You can however tell Murus to avoid using stateful inspection selecting the "Static filtering" option for Managed Inbound Services. You can also add custom rules using the "no state" PF option.

Murus PF States Inspector

Click the “Tools” button in Murus main window toolbar then click the “Inspector” button to open the PF States Inspector window.

Click the Update button in PF States Inspector window toolbar to display the list of currently active PF states.

	Kill All States	Sort by source address ↕	Show only established ↕	Update
tcp	192.168.2.2 50065 ->	17.158.8.86 993	ESTABLISHED:ESTABLISHED	
tcp	192.168.2.2 50067 ->	17.158.8.86 993	ESTABLISHED:ESTABLISHED	
tcp	192.168.2.2 50068 ->	17.158.8.86 993	ESTABLISHED:ESTABLISHED	
tcp	192.168.2.2 51521 ->	192.168.2.1 22	ESTABLISHED:ESTABLISHED	
tcp	192.168.2.2 51522 ->	192.168.2.1 5900	ESTABLISHED:ESTABLISHED	
tcp	192.168.2.2 548 <-	192.168.2.1 49334	ESTABLISHED:ESTABLISHED	

Each row represents a PF state. In the example shown above we see six PF states, each one representing an active network connection. We see five outbound connections to MAIL, SSH and VNC services, and one inbound connections to local AFP service (port 548). All connections take place between two different hosts, from and to specific TCP ports.

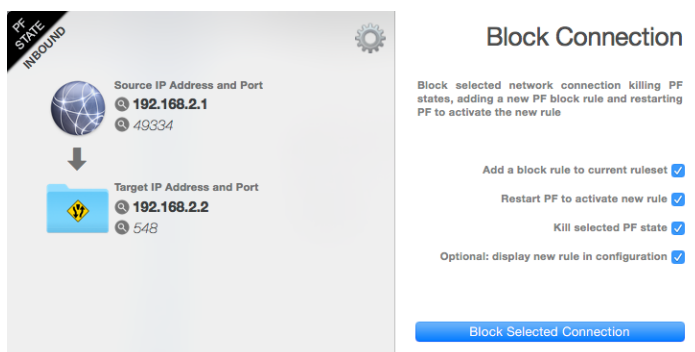
In case of a NAT connection PF state seen from a Mac running Murus and acting as a dual homed router, the connection will have three different hosts: the client, the router and the server, like shown in the screenshot below.

tcp	193.162.146.4 21 <-	10.0.0.2 49634	ESTABLISHED:ESTABLISHED
tcp	10.0.0.2 49634 ->	192.168.2.2 44075 ->	193.162.146.4 21 ESTABLISHED:ESTABLISHED

By default Murus shows only states with the ESTABLISHED status. It means the state is active. You can tell Murus to display all states including closing and idle states. Select the popup button in PF States Inspector window toolbar and choose “Show all connections”. You can sort PF states using the other popup button on the left.

To kill all PF states click the “Kill All States” button in the toolbar. This will close all active connections that relies on PF states.

State Inspector Info Popover



You can further inspect each PF state by double-clicking it. A new popover view will appear, showing some options for selected state.

Click the magnifier buttons to get info about selected IP address and ports.

Blocking a connection

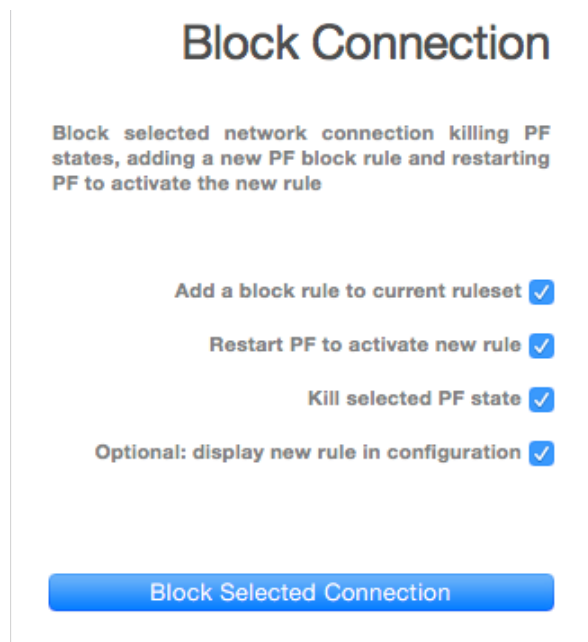
The right side of the State Inspector popover view is the place where you can block selected connection.

Blocking a connection is a three steps procedure:

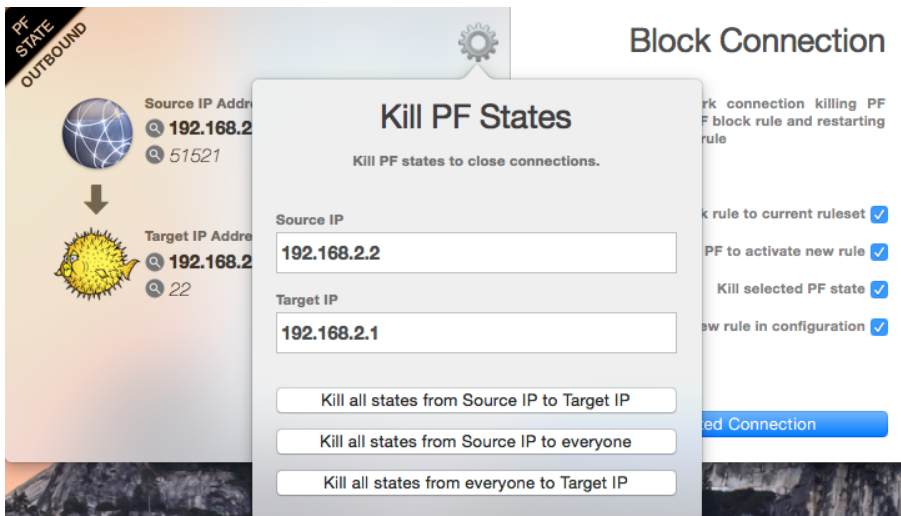
- 1) add a block rule to Murus ruleset
- 2) restart PF to activate the new rule
- 3) kill the PF state to close current connection

There is a fourth optional step, to display the newly created block rules in Murus PF Expanded Configuration window.

In some cases you may want to disable some of these steps, according to your needs. For example you may want to issue a block rule for the future, but do not want to kill current connection, so you uncheck the “Kill selected PF state” button.



Kill PF States



Click the ‘gear’ button in State Inspector popover view to open the PF States Killer view. You have three buttons to choose from. **Each buttons kills all states matching a specific pattern.**

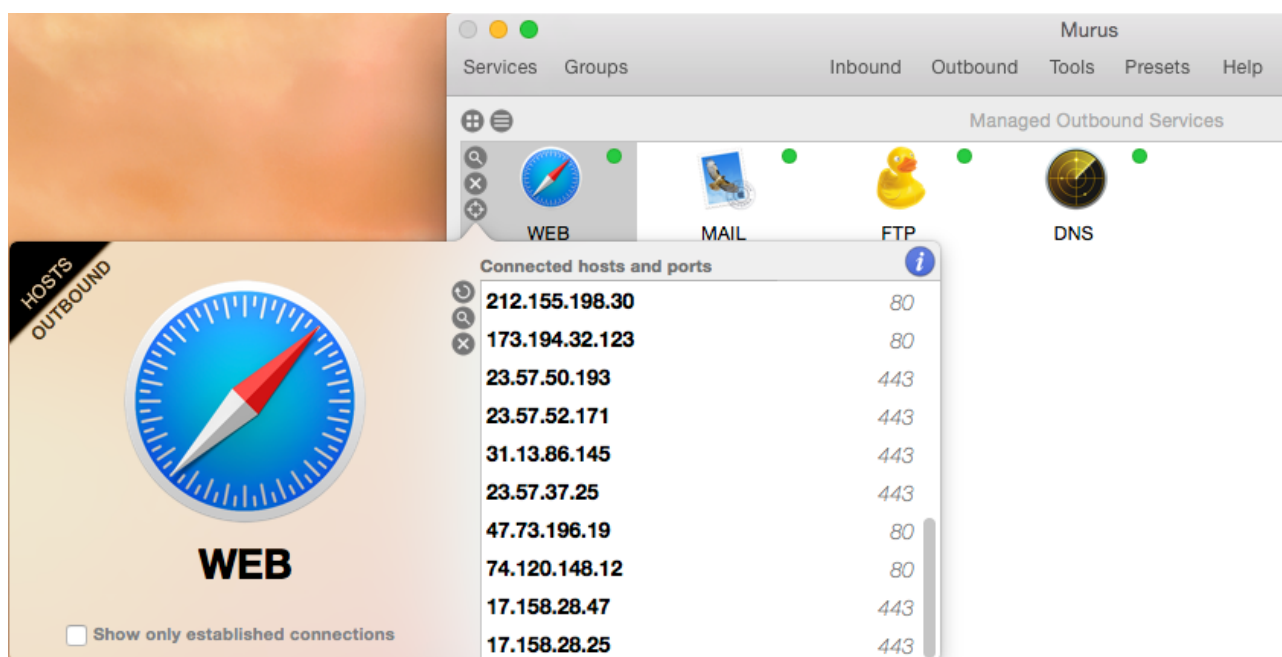
Source and destination IP are directly taken from the selected PF state, but you can edit them in this view. Every time you click one of these three buttons, the PF States Inspector main window will update. Please note that this panel is used only for closing PF states. No PF rule will be added to Murus ruleset.

Service Hosts Inspector

Murus is able to display currently connected hosts for each managed service, in both Managed Inbound Services and Managed Outbound Services views.

Connected remote IP addresses are taken from currently active PF states, so this list is limited to addresses involved in connections for which a PF state has been created. So if you enable static filtering for a service, connected hosts will not be visible in the Service Hosts Inspector view.

To open the Service Hosts Inspector view select a Murus Service in Managed Inbound/Outbound Services view and click the “sight” button.



You may choose to display only ESTABLISHED connections or all connections. Select an IP address and click the magnifier icon to display DNS, WHOIS and GEOIP information for that IP.

Clicking the “X” button does the following:

- INBOUND: kills all states originating from selected IP and targeting everyone;
- OUTBOUND: kills all states originating from everyone and targeting selected IP.

Please note that this “Kill” button will kill all selected IP’s connections, not only connections for selected service.

Section 7

NAT and Port Forwarding

Share your Internet connection with other computers, tablets or smartphones using Murus NAT. Learn how to limit Internet access for clients and how to export LAN services.

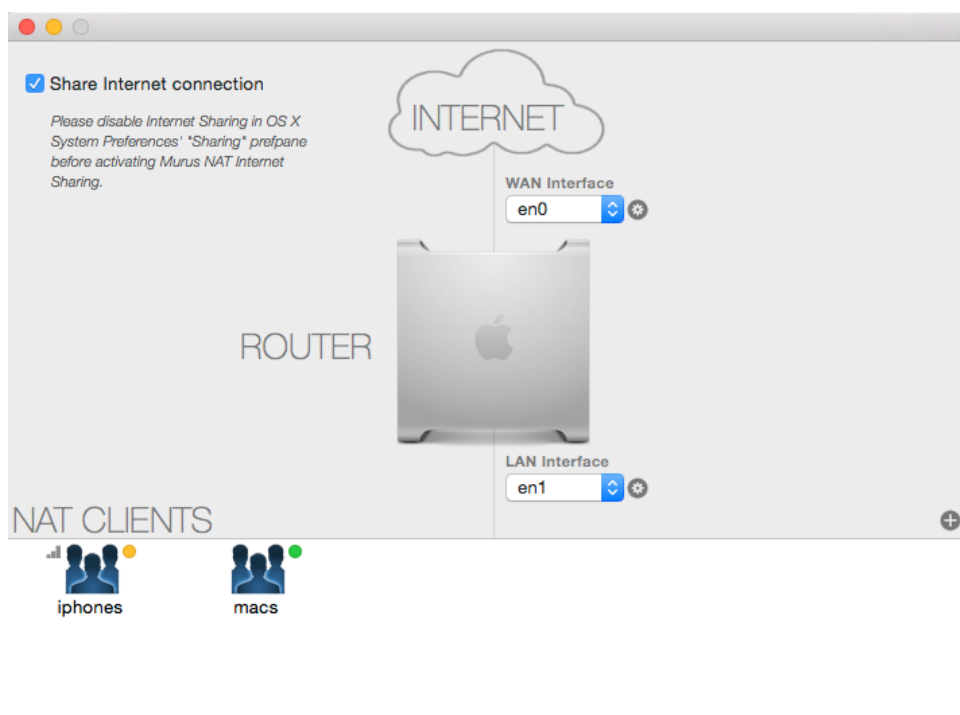
Share your Internet connection

You can configure your Mac as a dual-homed router in order to share your Mac's Internet connection and VPN connection with other computers, tablets, smartphone and such. Normally you do it activating the "Internet Sharing" service in OS X System Preferences - Sharing panel. But Murus offers an alternative way to do the same thing, with many more options. Using Murus you will be able to share your Internet connections with per-client and per-service rules, increasing security of both your Mac and your clients. You are also able to forward services from your client to the Internet using Murus port forwarding.

To share your Internet connection using Murus you need to disable the OS X Internet Sharing service in OS X System Preferences' "Sharing" prepane. This is mandatory because OS X Internet Sharing conflicts with Murus ruleset.

To activate Internet Sharing using Murus you need to configure Murus NAT.

Murus NAT



Click the "Tools" button in Murus main window toolbar and click the "NAT" button to open the Murus NAT window. This is the place where you configure general NAT settings and where you create NAT clients outbound rules.

To properly configure Murus NAT you have to:

- 1) **Select the correct WAN and LAN network interfaces (up to 3 LANs, including VLANs)**
- 2) **Optionally share your VPN connection with NAT clients, select the pop interface**
- 3) **Create NAT Groups (LANs hosts can be mixed)**
- 4) **Assign IP addresses and Services to NAT Groups**
- 5) **Optionally forward DNS queries to your default DNS**
- 6) **Optionally block traffic from NAT clients to WAN services (safer)**
- 7) **Check the "Share Internet connection" button in NAT window**

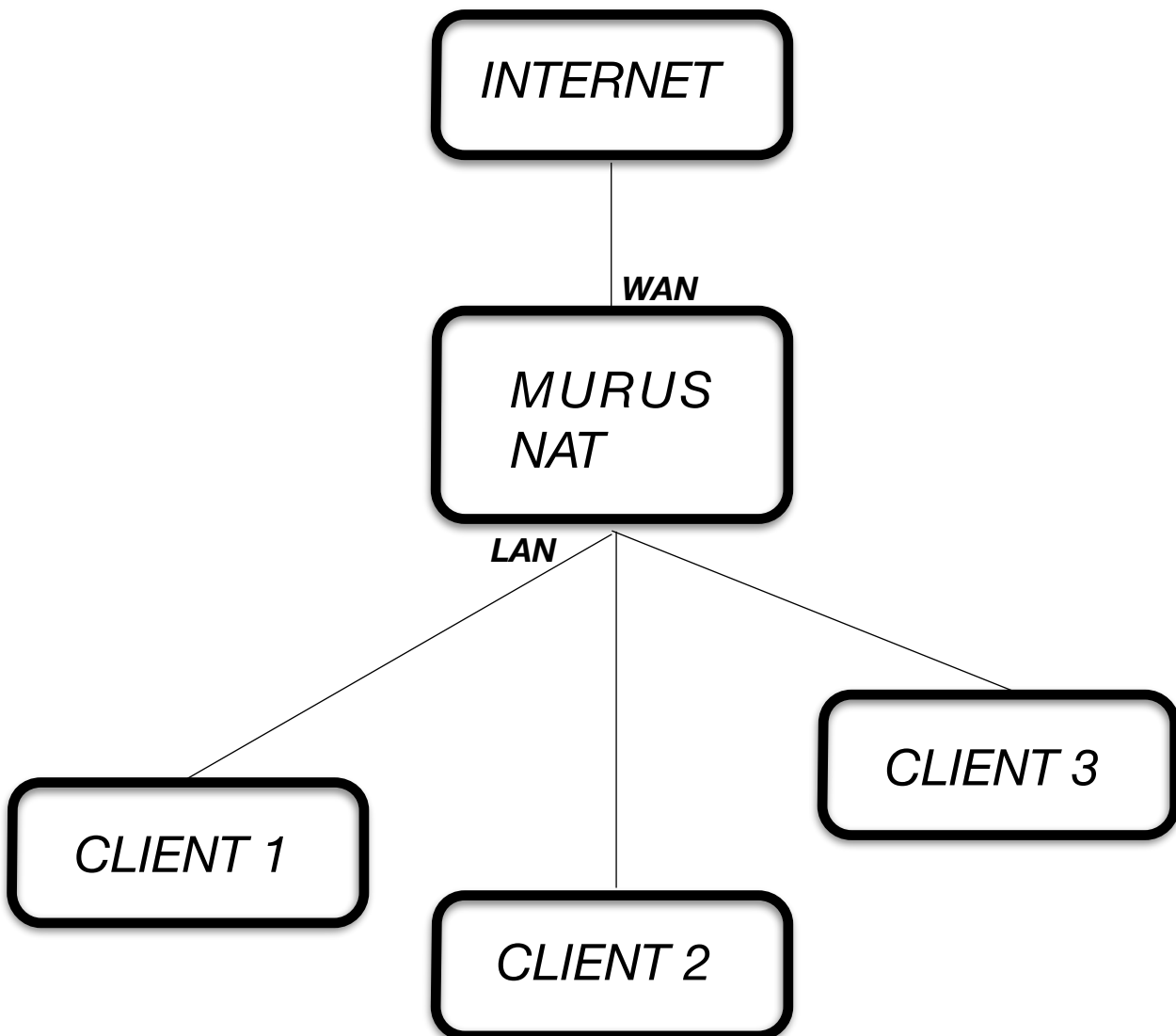
To export services from the LAN you have to activate and configure port forwarding. This is done in the Managed Inbound Services views. This topic has been covered in a previous section of this manual.

WAN and LAN network interfaces

A basic dual-homed router needs at least two available network interfaces. The WAN interface is the one connected to the Internet, usually featuring a public IP address (but it can also be a private one).

The LAN interface is the one connected to the local network. It features a private IP address and it is “seen” by other computers in your local network. These computers will use your LAN interface IP address as router address. Murus supports up to 3 different LANs, including VLANs.

Here is an example of dual-homed configuration on a computer running a public IP address:



In this example the WAN interface has a public IP address, but you can use the same configuration if your Mac is behind a NAT router and it is using private IP addresses on both interfaces.

Click the small round button to open the Interfaces popover. Here you see all available network interface.

Interface	IPv4 Address	IPv6 Link local Address	IPv6 Address	MAC Address	Hardware Port
lo0	127.0.0.1	::1	fe80::1		
gif0					
stf0					
en0	192.168.2.2	fe80::225:ff:fef1:4614		00:25:00:f1:46:14	Ethernet 1
en1				00:25:00:f1:9d:e2	Ethernet 2
fw0					FireWire
pflag0					
vlan0	10.0.0.1	fe80::225:ff:fef1:4614		00:25:00:f1:46:14	

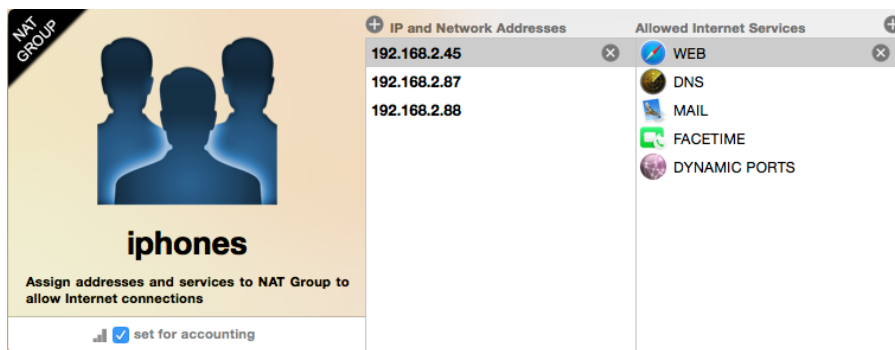
Murus NAT window has two popup button. The upper is used to set the WAN interface, while the lower is used to set the LAN interface.

NAT Groups

The bottom side of NAT window shows a white empty area. This is the place where all your NAT Groups are stored. Click the small “•” button to add a NAT Group.

A NAT Group is a Murus object defined by an icon, a name, a list of IP and/or Network addresses and a list of Murus Services.

Choose a name for the new NAT Group then click “•” to add it. Its icon will appear in the NAT Groups view. Select its icon and click the magnifier button to open the NAT Group edit popover.



NAT Group edit popover.

Here you see two empty columns and two “•” buttons. On the left side you have to add IP addresses of NAT clients. On the right side you need to

add services allowed for selected NAT Group. Clients listed on this group will be able to access only these services on the Internet. All other services will be blocked. So, for example, if you want your client to be able to browse web sites you should add the WEB service. To give unrestricted Internet access to your

clients you have to add the ALL SERVICES service. If you want you can activate traffic counters checking the “set for accounting” option. The NAT Group will show a green, yellow or red according to its access rights. An address may be contained in more than one NAT Group. Click “Start” in Murus main window toolbar to apply changes every time you modify NAT settings.

NAT Blocking policy

NAT clients should not be able to connect to services running on the router (the Mac running Murus NAT) unless specified by assigning specific groups to specific services in the Managed Inbound Service area.

NAT client may be able to connect to the router to both WAN and LAN side. LAN side can actually be more than a interface. With Murus up to three LAN interfaces can be configured, and many more can be physically active on the Mac.

- Traffic from NAT clients to services running on router’s WAN interface:

This traffic can be blocked setting the “Block access to WAN from LAN” option in Murus NAT window.

- Traffic from NAT client to services running on router’s LAN interfaces:

This traffic is blocked by the default Murus blocking rule. Traffic from NAT clients is allowed to any destination excluding destinations included in the <NatLanInterfaces> PF table. Murus automatically puts in this PF table all LAN interfaces set in the Murus NAT window.

Section 8

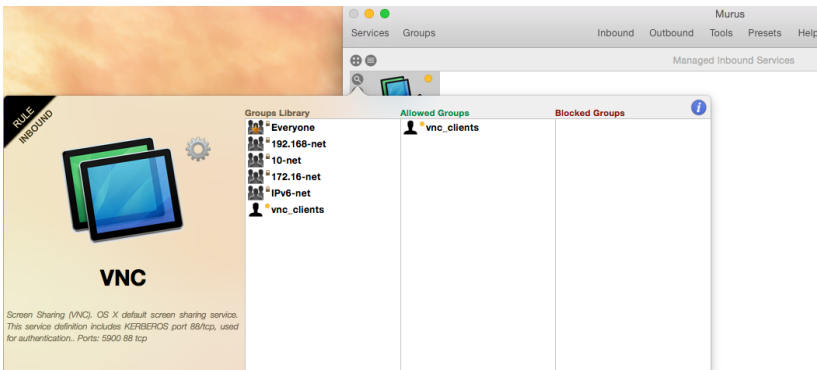
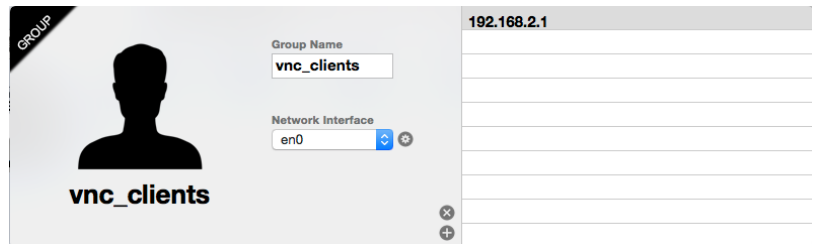
Murus logic by examples

Example 1: Dealing with PF States

By default Murus uses PF states to pass inbound and outbound connections to local and remote services.

In this example we want to show how PF states affects networking. We use a very simple firewall configuration where we want to allow inbound connections from a remote computer to our Mac's VNC service (Screen sharing).

First of all we create a new group named "vnc_clients" and we add the "192.168.2.1" address. Then we bind it to our Mac's en0 interface, which is the primary ethernet interface in this case, with IP address 192.168.2.2. This group will appear with a yellow dot, meaning that it is bound to an interface.



We want to allow connections from this group to our Mac's VNC server, so we select the "Managed Inbound Services" view, we remove all services icons clicking the "X" button, and then we add the VNC service.

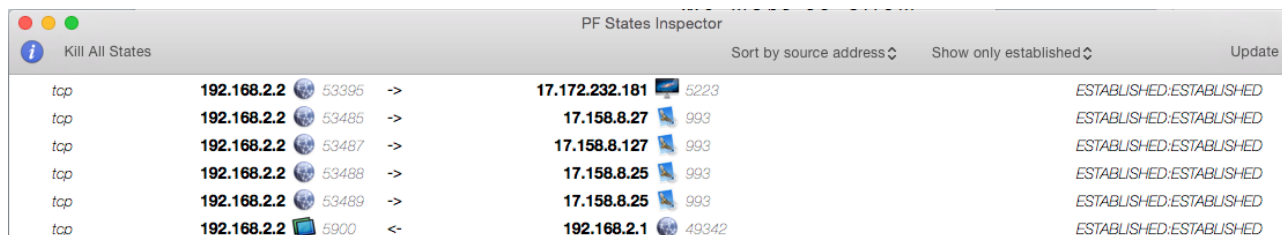
Then we click the magnifier button to open the Inbound Rule popover, and we assign the "vnc_clients" group to the VNC's "Allowed Groups" column. The service led will turn from green to yellow, meaning that its access is restricted only to a limited number of IP addresses. In our case only one IP address.

As you see, VNC is the only service listed in Managed Inbound Services view, so all other services are blocked.

We click the "Start" button in Murus main window toolbar to reload PF firewall rules, to activate this new ruleset.

Now we make the VNC connection. We do a real VNC connection from the remote Mac using the OS X built-in screen sharing client. Once done, keep the VNC connection open on the remote side and switch back the focus on the Mac router running Murus.

Now we open the Murus PF States Inspector window to check current active connections.



Protocol	Local IP	Local Port	Direction	Remote IP	Remote Port	State
tcp	192.168.2.2	53395	->	17.172.232.181	5223	ESTABLISHED:ESTABLISHED
tcp	192.168.2.2	53485	->	17.158.8.27	993	ESTABLISHED:ESTABLISHED
tcp	192.168.2.2	53487	->	17.158.8.127	993	ESTABLISHED:ESTABLISHED
tcp	192.168.2.2	53488	->	17.158.8.25	993	ESTABLISHED:ESTABLISHED
tcp	192.168.2.2	53489	->	17.158.8.25	993	ESTABLISHED:ESTABLISHED
tcp	192.168.2.2	5900	<-	192.168.2.1	49342	ESTABLISHED:ESTABLISHED

As you can see in the screenshot above, the last state grants inbound connections from remote IP address 192.168.2.1 to our Mac's IP address 192.168.2.2 on port 5900 (the VNC Screen Sharing port). This state has been dynamically created by PF when the remote VNC client got access to our local VNC server. The arrow displays a "left direction", meaning that the initial connection has been made from a remote host, so it is considered an inbound connection. Despite that, this state allows VNC traffic between these two hosts in both directions.

Now we go back to the main Murus window, in the Managed Inbound Services view. We do remove the VNC service from this view, in order to tell Murus to block it. Then we click "Start" in the Murus main window toolbar to reload PF rules and activate the new ruleset.

Now every attempt to connect to our running VNC server will be blocked.

But what about the existing connection? Is it blocked? Dropped? Closed? **NO IT ISN'T.**

Current active rules deny access to local VNC server, and this is true, but existing states are preserved, so the VNC connection is still alive. This connection has been initiated when these kind of connections were allowed. For this reason the connection will stay alive until the client and/or the server decides to close it. This is true for TCP connections. UDP states will close using timeouts.

Click "Update" in PF States Inspector window toolbar to refresh the PF states table. You should see the VNC state is still there.

It is mandatory to understand this PF States behavior because this affects PF testing and troubleshooting. Some time it is a good practice to "Kill All States" before reloading PF rules clicking "Start" button, in order to test them starting from a clean PF states table. Please note that killing a state will close connections but in some cases some clients/servers applications may try to restore it immediately after.

Example 2: Rules Order

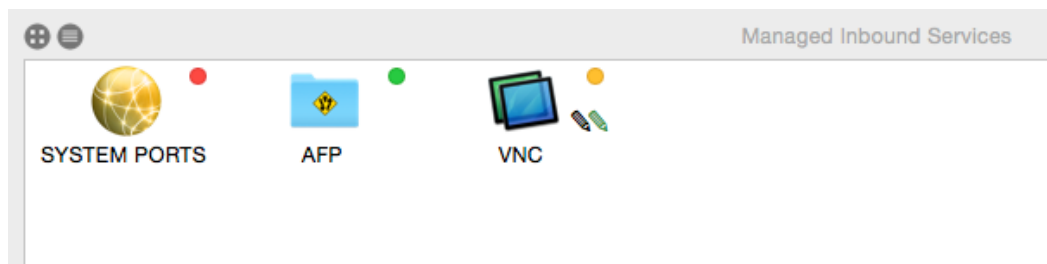
Rules order matters. You already know that, if you read the previous sections of this manual. “Last matching rule wins unless a packet is matched by a rule with the quick keyword”.

In this example we show how Murus Services icons order affects the overall PF ruleset generated by Murus. Our simulated environment is the typical home network with a DSL router connected via ethernet (or wifi) to our lone Mac in a single-host network. We set up the DSL router to forward all traffic to our Mac, in order to fully expose our Mac’s network interface to the Internet. All TCP and UDP traffic from port 1 to port 65535 is redirected to our Mac.

Before activating this configuration you should disable all services in OS X System Preferences - Sharing prepane. We will activate a service later, for testing purposes.

Now open Murus. We assume that Murus Preferences are set with default values. To restore Murus default configuration you can use at any time the Murus menu -> Firewall -> Restore Default Murus Configuration.

Select the Managed Inbound Services view and drag SYSTEM PORTS, AFP and VNC services icons from the Services Library. Delete all other services, if there is any. See screenshot below.







Click the magnifier button to configure the three services as follows:

SYSTEM PORTS: assign group “Everyone” to “Blocked Groups” and leave “Allowed Groups” empty. Click the “gear” button and deselect all options.

AFP: assign group “Everyone” to “Allowed Groups” and leave “Blocked Groups” empty. Click the “gear” button and deselect all options.

VNC: assign group “192.168-net” to “Allowed Groups” and leave “Blocked Groups” empty. Click the “gear” button and select only “log blocked connections” and “log allowed connections” options.

Now open the Murus Expanded PF Configuration window and look at the ruleset:

- ▼  block in proto {tcp, udp} from any to any port {1:1023}
- ▼  pass in proto tcp from any to any port {548 88} flags S/SA keep state
- ▼  block in log proto tcp from any to any port {5900 88}
- ▼  pass in log proto tcp from <192.168-net> to any port {5900 88} flags S/SA keep state

The rules shown in the screenshot above are generated by the Services icons you just added to the Managed Inbound Services view.

What's the effect of this ruleset? We will see it from two points of view:

filtering and **logging**.

- *Filtering*

From a filtering point of view you have to consider that, by design, Murus blocks all connections except those explicitly allowed to pass. And the Managed Inbound Services view is exactly the place where you do that. So if this view is empty, no inbound connections is allowed. This very basic behavior cannot be changed.

So, we have three services in this view at the moment. Let's look at their properties, focusing in their Ports Range:

SYSTEM PORTS: 1:1023 (it means all ports from port 1 to port 1023)

AFP: 548

VNC: 5900

You should notice that service AFP is "included" into service SYSTEM PORTS (because AFP port 548 is included in the range from 1 to 1023), while service VNC is not. This is important because rules generated by service AFP override rules generated by service SYSTEM PORTS. You can clearly see it in the screenshot above: AFP rule comes after SYSTEM PORTS rule. So if a packets matches both rules, the AFP rule will win, and will decide what to do with the packet. In this case, as it is a pass rule, it will pass all inbound AFP connections. The practical effect of this ruleset is:

SYSTEM PORTS: this icon has no filtering effect in this case, because it blocks ports that were already blocked by the default Murus filtering policy. Being the first service in list, it is not able to override rules generated by other services. So in this particular scenario this service has no effect on filtering.

AFP: this icon actually has the effect to allow connections from all remote hosts to local AFP File sharing service. This "pass" rule is not override by any of the forthcoming rules so is the one that wins.

VNC: this icon actually has the effect to allow connections from some remote hosts (192.168-net group) to local VNC File sharing service. This "pass" rule is not override by any of the forthcoming rules so is the one that wins.

- Logging

From the logging point of view you have to consider that:

- Murus default policy for allowed connections is to ignore logging them, and this behavior cannot be changed.
- Murus default policy for blocked connections is to log all of them, but this can be changed in Murus Preferences “General” tab.

Now we are using a ruleset with default preferences, so we assume that the option “**Log all blocked connections**” in Murus Preferences - General - is correctly checked. We assume also that the “**Inbound per-service block rule**” is checked in Advanced tab. More about this option in the next example.

So the default behavior of the ruleset in this example is to log all inbound blocked connections.

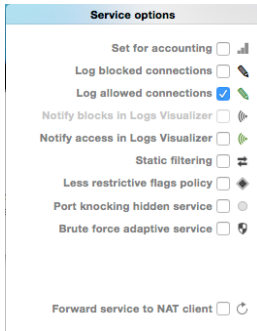
What’s the effect of the three Services icons on the PF logging system?

SYSTEM PORTS: this Service icon lacks the black pencil icon, so it means that the “log blocked connections” option is disabled. This has the effect to override the default logging policy for ports included in this service. Blocked connections to services in the 1:1023 port range will not be logged, according to this rule.

AFP: this Service icon generates only pass rules. It lacks the green pencil icon, meaning that allowed connections are not logged. This does not override the global policy because allowed connections are not logged by default. So this Service icon has no effect on logging.

VNC: this Service icon generates both pass and block rules. It has both the black pencil and the green pencil icons, meaning that both blocked and passed connections will be logged. While this does not override global blocked connections logging policy, it overrides the global passed connections logging policy.

Example 3: Inbound per-service block rule option

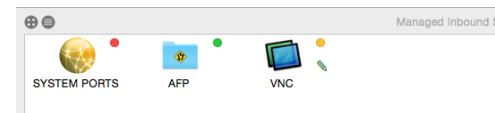


Following the example above, we have to do a small change in the ruleset in order to explain how this option affects filtering and/or logging.









Select Managed Inbound Service view, select VNC service, click the magnifier button to open the Inbound Rule popover, then click the ‘gear’ button to open the Service Options popover.

Deselect the “Log blocked connections” option.

Click “Start” button in the toolbar to reload PF rules.









Now look at Expanded PF Configuration window:

-   block in proto {tcp, udp} from any to any port {1:1023}
-   pass in proto tcp from any to any port {548 88} flags S/SA keep state
-   block in proto tcp from any to any port {5900 88}
-   pass in log proto tcp from <192.168-net> to any port {5900 88} flags S/SA keep state

The first VNC rule (third rule shown in screenshot above) has changed, now it lacks the “log” option. This rule now overrides the global logging policy: blocked VNC connections will not be logged. Passed VNC connections will still be logged.

Activating the “Inbound per-service block rule” option

Now to understand the effect of “Inbound per-service block rule” please open Murus Expanded PF Configuration window then open Murus Preferences and select Advanced tab. Keep both windows visible. In Preferences window uncheck the “Inbound per-service block rule” option and see the effect it has on the PF

-   block in proto {tcp, udp} from any to any port {1:1023}
-   pass in proto tcp from any to any port {548 88} flags S/SA keep state
-   pass in log proto tcp from <192.168-net> to any port {5900 88} flags S/SA keep state

configuration:

Now the VNC service icon generates only one rule instead of two.

The missing VNC rule is a block rule.

When “Inbound per-service block rule” option is selected, **this block rule is generated by every service icon featuring the “yellow led”**. This block rule is used to “restore” the default filtering blocking policy on a per-service basis, at the beginning of every “group of rules” generated by a each services icons.

In this specific example, disabling the “Inbound per-service block rule” option has no effect on filtering but has an effect on logging: now blocked VNC connections will be logged because inbound VNC packets will match the global blocking rule, and, in this example, Murus Preferences are set to log all blocked connections.

“Outbound per-service rule” option has the same effect on outbound rules.

Example 4: Logging and Notifications

In this example we want to show the logging capabilities of PF and the interaction between Murus and Murus Logs Visualizer. Our scenario is the same as previous example: a typical home network with a DSL router and a ethernet/wifi connected Mac behind router's NAT, using a single private interface on the 192.168-net network address space. All TCP and UDP traffic is redirected from the router public interface to the Mac's interface, which is fully exposed to the Internet.

We want to setup Murus in order to monitor remote attempts to hack into our Mac using vulnerabilities for very common network services like SSH, TELNET, MYSQL, APACHE, and such. We focus only in inbound filtering, assuming no outbound filtering is configured.

We want the logging system to be as much focused as possible on our targets, being less verbose as possible. We need to build a sort of "statistically valid" log report in order to understand what services are currently targeted by hackers and script kiddies.

What are they doing?

Before going deep into Murus configuration, we want to give you some information on how these "hackers" do to their job. Most of them simply follow a very simple and common pattern made of these steps:

- 1) focus on a specific service for which they have a working remote exploit
- 2) mass scan the Internet for hosts running such services and build a list of IP addresses
- 3) filter IP list selecting hosts running the specific vulnerable version of this service
- 4) get unauthorized root access to these host using the exploit
- 5) filter IP list selecting "interesting" hosts (hosts with static public IP, high bandwidth, plenty of disk space, lazy admin, the right OS, and such)
- 6) install a rootkit or a backdoor in order to grant an easier and more robust way to take control of hacked host over time
- 7) patch the vulnerable service to avoid other hackers to "steal" the hacked host.
- 8) steal databases or install every sort of lame software for lame activities. Hacked hosts may be used for every purpose, including being part of spam nets, bot nets and scan nets or hosting "deep web" barely legal hidden tor services. They can also be used as honeypots: hackers putting traps for other hackers with the purpose of stealing 0day tools or access to hacked shells and/or services/nets.

They do this 24/7, and they are going to do this 24/7 for the next centuries.

What are we going to do?

It is your duty to understand that running a firewall is not enough to secure a computer connected to a network. The firewall is only a part of a very complex system. Shutting down unused services, doing security updates and using good passwords, for example, are as important as correctly configuring the firewall.

Anyway the purpose of this manual is to explain how Murus and PF work, so we will focus only on this topic.

We are going to try to stop their task list at the very beginning, because we are going to block ALL connections to ALL our services. Their attempt to discover running services will simply fail, mainly for two reasons:

- 1) we are clever enough to turn off our potentially vulnerable network services, so there are no listening ports on our side.
- 2) we are going to use a firewall that blocks all inbound connections, so if we forgot to (or we can't) close a service, access to this service will be denied by the firewall.

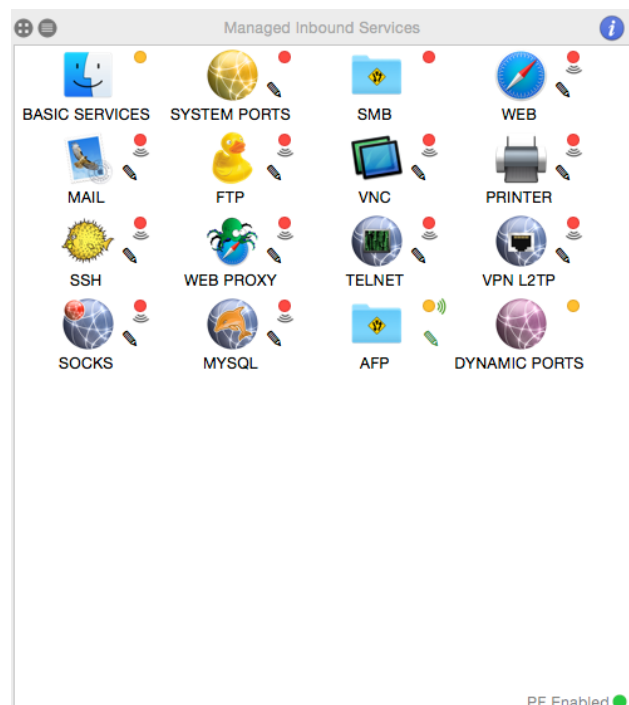
We assume that Murus Preferences are set as default except for the logging policy. Go to Preferences - General and uncheck the “Log all blocked connections” option.

Look at the screenshot, this is the Managed Inbound Services view. It contains 16 icons.

We see 3 icons with the yellow led:

- **BASIC SERVICES**
- **AFP**
- **DYNAMIC PORTS**

connections to these services are allowed only from the LAN, because we assigned the group “192.168-net” to their “Allowed Groups”, and we left their “Blocked Groups” empty. Service AFP is set to log passed connections and to notify them with Murus Logs Visualizer.



Then we see 13 icons with a red dot. This is the interesting part.

These services has the “Everyone” group assigned to “Blocked Groups”, while we left all “Allowed Groups” empty.

Adding these icons has no effect on filtering, as you may guess, because all these services were already blocked by the Murus global blocking rule. So these icons affect only logging. While we disabled global logging on blocked packets, these services (actually only 12 services out of 13) has the black pencil icon, meaning that blocked connections will be logged, and they are also set to notify these blocks in Murus Logs Visualizer, as underlined by the black wave icon.

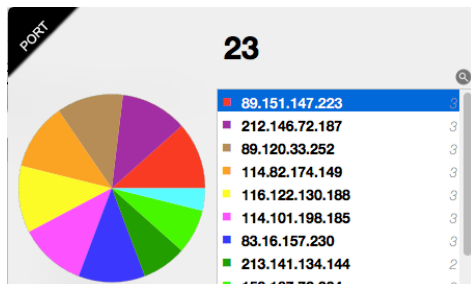
Click “Start” to apply this ruleset. The effect of this ruleset is:

Ports	Addresses
23	89.151.147.223
22	212.146.72.187
3128	114.101.198.185
80	46.36.35.233
3306	114.82.174.149
8080	89.120.33.252
53	83.16.157.230
25	116.122.130.188
135	178.19.104.247
161	103.41.124.60
623	74.208.126.139
443	153.187.72.204
	213.141.134.144
	124.232.142.220
	66.240.236.119
	122.224.71.50
	218.2.0.130
	119.195.42.173
	117.27.158.69
	122.225.97.70
	60.173.14.67
	43.240.237.15
	174.139.105.122
	125.75.128.136
	88.249.121.158
	125.46.40.22
	134.147.203.115
	216.99.158.68
	62.210.93.52
	93.174.93.218
	222.186.56.46
	221.194.44.151
	115.239.248.48
	204.42.253.2
	104.194.19.11
	222.186.21.66

- Accept connections only from local LAN 192.168-net network to BASIC SERVICES, AFP and DYNAMIC PORTS
- Block ALL inbound connections to ALL services from the Internet
- Log attempts to connect to ALL system ports (from port 1 to port 1023)
- Log attempts to connect to 12 local services featuring the black pencil. Some of them is already included in the 1:1023 range, but we need to add their icons in order to activate also the notification system.
- Notify attempts to connect to some of these services in Murus Logs Visualizer using OS X notification system.

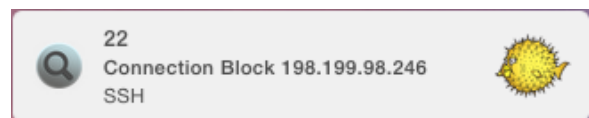
After some time (2-3 hours), here is an example of Murus Logs Visualizer realtime report. Look at the screenshot on the left.

On the left column you see the list of blocked ports, on the right side the list of blocked IP addresses.



We see that the most attacked port is port 23. This is the port for TELNET service. We may further investigate the activity on this port clicking a button and showing the list of remote IP addresses that tried to get into our TELNET service. Addresses are sorted by number of attempts.

On the right an example of a notification by Logs Visualizer. We see that a remote IP address just tried to scan our port 22 for SSH service. The connection has been blocked.



For more information about PF please see the Murus OS X PF Manual, available at www.murusfirewall.com/support

© 2014-2015 muruset

by *The Murus Team*

www.murusfirewall.com

info@muruset