Transparent Firewall/Filtering Bridge - pfSense 2.0.2

By William Tarrh

Version 2 – February 6, 2013

Transparent Firewall/Filtering Bridge - pfSense 2.0.2

This “how to” is an updated version of Trendchiller’s 2007 *How to Setup a transparent firewall /filtering bridge with pfSense* based on **pfSense 1.0-PREBETA2-BUG-VALIDATION-EDITION**.

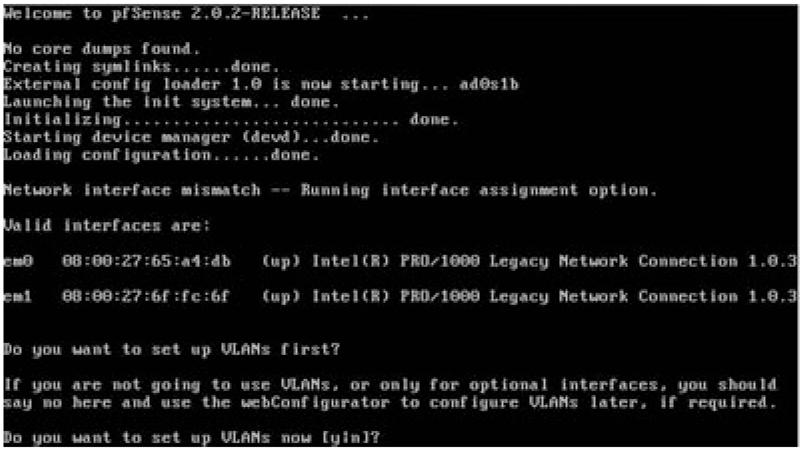
My contribution to this project is documenting what has been noted by others on the pfSense forum, walking in Trendchiller’s footsteps and the submission of the document itself.

Special thanks to Chris Buechler, Scott Ullrich and all of those who contribute to the pfSense Forum. I would also like to thank Dr. Jeff Rattray who helped me work through some of the kinks in this project.

Contents

1. **Hardware Requirements and Setup**
   a. Two compatible NIC's for the LAN and WAN interfaces.
   pfSense Hardware Compatibility

2. **Initial Setup**
   a. Upon completing a fresh installation of pfSense a restart will be required. After the first reboot you will be greeted with **"Do you want to set up VLANs now [y|n]?"** Select **"No"**.



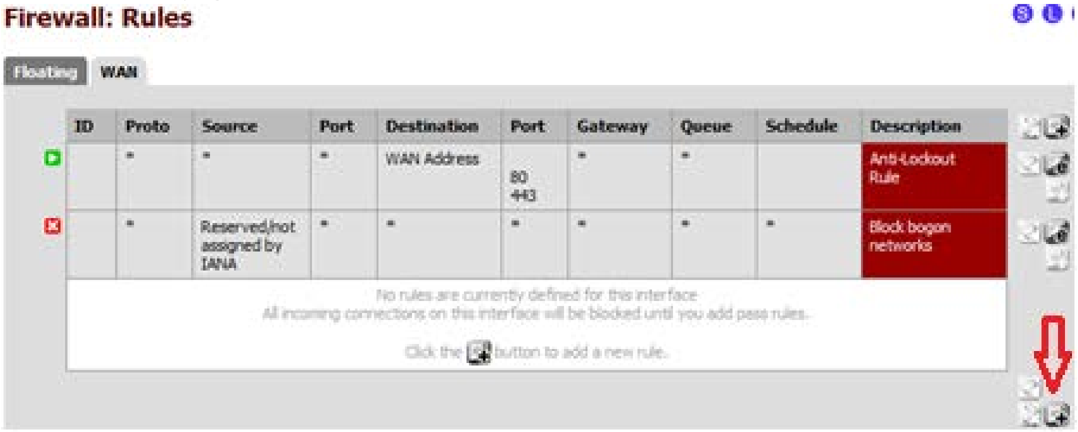
```
Welcome to pfSense 2.0.2-RELEASE  ...

No core dumps found.
Creating symlinks......done.
External config loader 1.0 is now starting... ad0s1b
Launching the init system... done.
Initializing............................ done.
Starting device manager (devd)...done.
Loading configuration......done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

em0   00:00:27:65:a4:db   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3

em1   00:00:27:6f:fc:6f   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3


Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?
```

   b. Next you will be requested to select your **WAN** interface or select **'a'** for auto detection. Select your desired **WAN** interface card from the list. Next you will be asked to select your **LAN** interface card. Press **"Enter"**, we will configure this interface later.
   c. At the welcome screen only setup the **WAN** interface. Assign this adapter a static address or use the assigned DHCP address; we will use this address to configure the firewall from this point on.

3. **pfSense GUI Login**
   a. Open a browser window and enter the IP address assigned to the pfSense **WAN** interface. The default username and password are **admin** and **pfsense**.

4. **Firewall – WAN - Anti-Lockout Rule**
   a. First, let's be sure not to get locked out of the **WAN** interface by setting up our own temporary "**anti-lockout**" rule. Navigate to **"Firewall" -> "Rules"**. By default the **"Anti-Lockout"** rule is applied to the **WAN** interface as seen below. As soon as the **LAN** interface is enabled this **"Anti-Lockout"** rule will be migrated automatically to the **LAN** interface.

b. To create a new rule, select the **'+'** on the bottom right-hand corner. This will take you to the **Rules: Edit** page**.**



Firewall: Rules

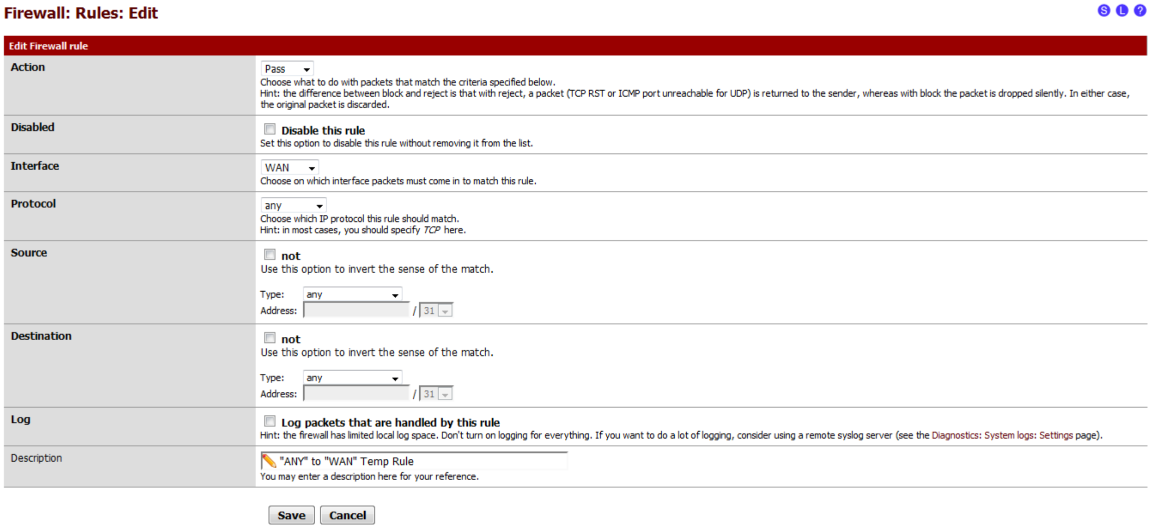
Floating | WAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
▶		*	*	*	WAN Address	80 443	*	*		Anti-Lockout Rule
☒		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

Click the button to add a new rule.

In the **"Rules: Edit"** create a rule that resembles the screen shot below. The rule below will allow all traffic to access the **WAN** interface. Keep in mind this is a temporary rule. Select **"Save"** and then **"Apply Changes"**.



Firewall: Rules: Edit

Edit Firewall rule	
Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	□ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose on which interface packets must come in to match this rule.
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ not Use this option to invert the sense of the match. Type: any Address: / 31
Destination	□ not Use this option to invert the sense of the match. Type: any Address: / 31
Log	□ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	"ANY" to "WAN" Temp Rule You may enter a description here for your reference.

Save | Cancel

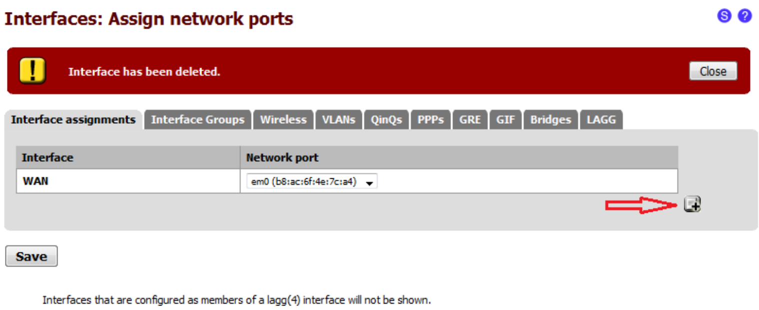
5. **Configure WAN Interface**

   a. Navigate to **"Interfaces" -> "WAN"** and scroll down to **"Static IP configuration".** In the **"Gateway"** field select **"add a new one"** and enter your Gateway.

   b. Navigate to **"System"** -> **"General Setup"**; add your hostname, Domain and DNS Servers. To the right of your DNS servers select your Gateway from the dropdown menus.

6. **Enable and Configure LAN Interface**

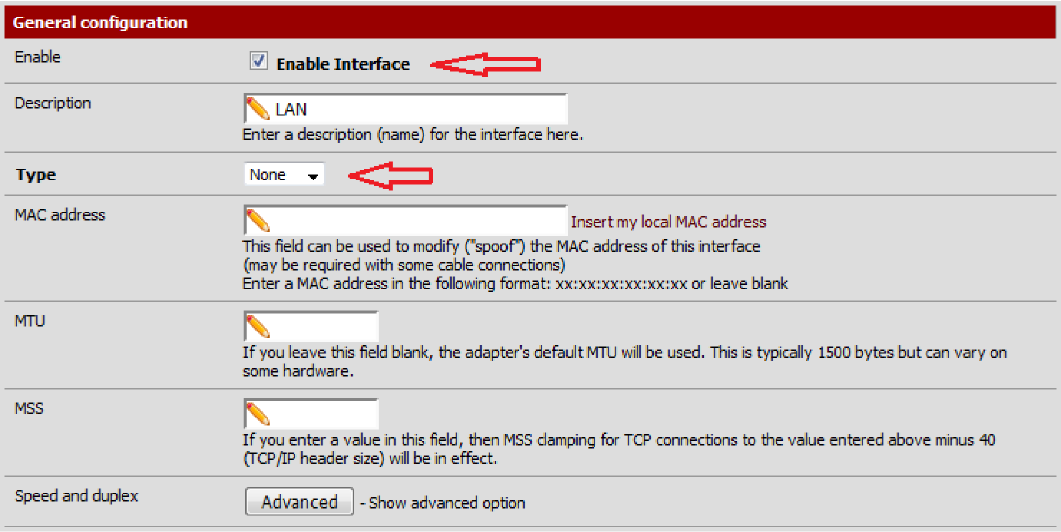
   a. Navigate to **"Interfaces" -> "(assign)"**. Select the **'+'** and then select your **"LAN"** interface. Now select **"Save"** and then **"Apply Changes"**.



Interface	Network port
WAN	em0 (b8:ac:6f:4e:7c:a4)

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Navigate to **"Interfaces" -> "LAN"**. In **General configuration** check the **"Enable Interface"** box. The screen will auto populate. Be sure that **Type** is set to **"None"**. **"Save"** and **"Apply Changes"**.



Enable ☑ Enable Interface

Description: LAN
Enter a description (name) for the interface here.

Type: None

MAC address: Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface
(may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

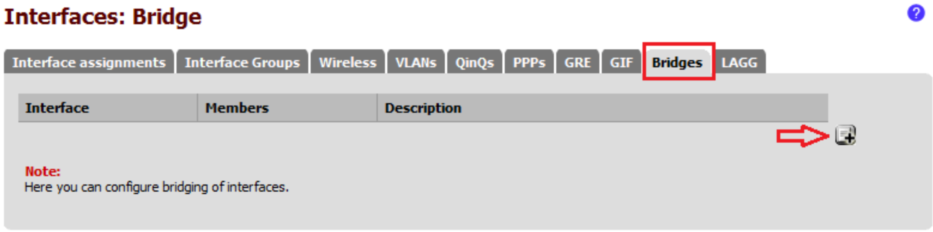
MTU: If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.

MSS: If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and duplex: Advanced - Show advanced option

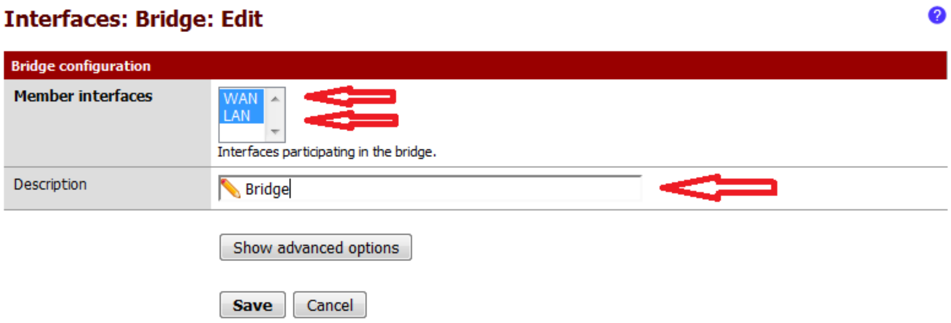
7. **Enable and Configure the Bridge**

   a. Now that our **LAN** and **WAN** interfaces are enabled and configured we can create the Bridge. Navigate to **"Interfaces -> (assign)"** from the menu and then select the **"Bridges"** tab to the far right. Select the **'+'** to navigate to **"Bridge:Edit"**.



Note:
Here you can configure bridging of interfaces.

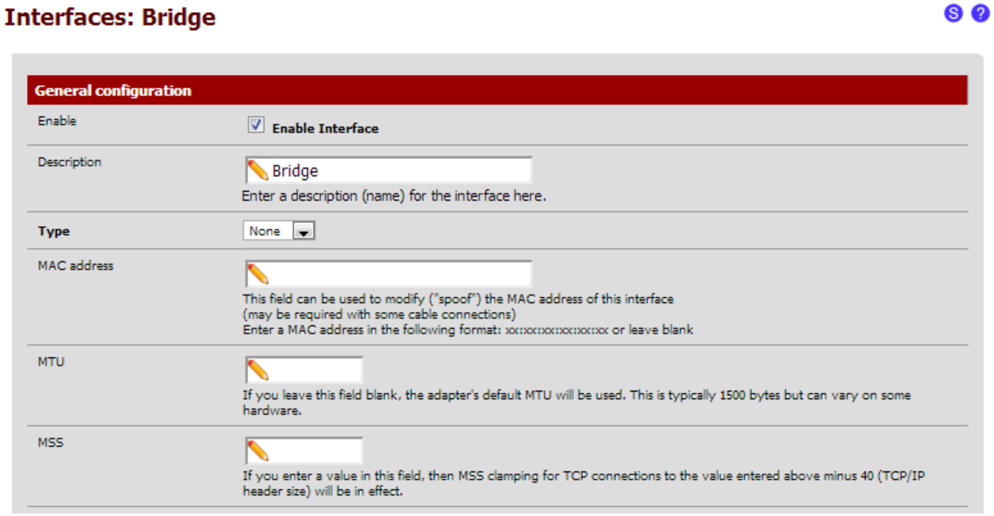
   b. In **"Bridge: Edit"** hold the **"Ctrl"** key on your keyboard and select the **"WAN"** and **"LAN"** so they are both highlighted. Assign your Bridge a name in the **"Description"** field. Select **"Save"** and then **"Apply Changes"**.



Interfaces: Bridge: Edit

Bridge configuration	
Member interfaces	WAN LAN Interfaces participating in the bridge.
Description	Bridge

c. Navigate to **"Interfaces" -> "OPT1"**. In **General configuration** check the **"Enable Interface"** box. The screen will auto populate. You can also change the interface description at this point, I have changed mine from **"OPT1"** to **"Bridge"**. Be sure that **Type** is set to **"None"**. **"Save"** and **"Apply Changes"**.



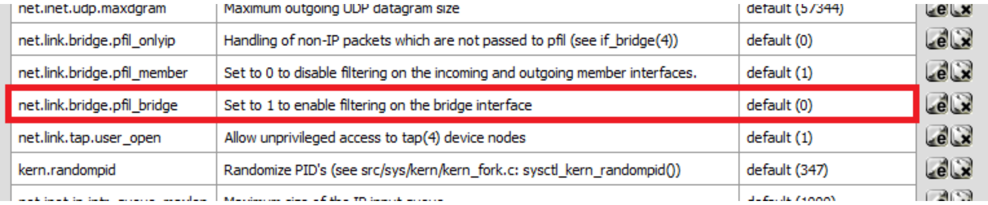
Interfaces: Bridge

General configuration	
Enable	☑ **Enable Interface**
Description	Bridge Enter a description (name) for the interface here.
Type	None
MAC address	This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

8. Enable the Filtering Bridge

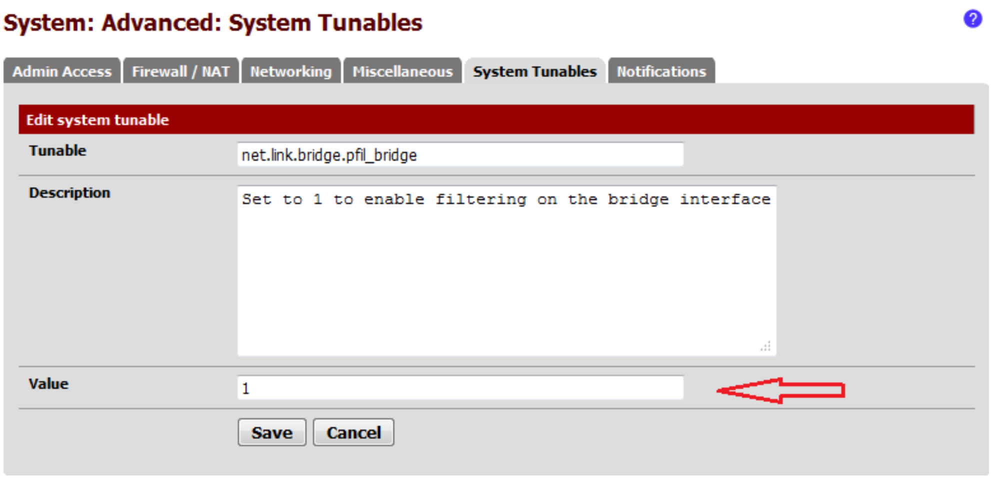
a. In the menu navigate to **"System -> Advanced"** and select the **"System Tunables"** tab.

b. Locate the **"net.link.bridge.pfil_bridge"** in the **"Tunable Name"** column and double-click it.



net.inet.udp.maxdgram	Maximum outgoing UDP datagram size	default (57344)
net.link.bridge.pfil_onlyip	Handling of non-IP packets which are not passed to pfil (see if_bridge(4))	default (0)
net.link.bridge.pfil_member	Set to 0 to disable filtering on the incoming and outgoing member interfaces.	default (1)
net.link.bridge.pfil_bridge	Set to 1 to enable filtering on the bridge interface	default (0)
net.link.tap.user_open	Allow unprivileged access to tap(4) device nodes	default (1)
kern.randompid	Randomize PID's (see src/sys/kern/kern_fork.c: sysctl_kern_randompid())	default (347)
net.inet.ip.intr_queue_maxlen	Maximum size of the IP input queue	default (1000)

c. In the **"Value"** field change this from **"Default"** to **"1"**. Select **"Save"** and **"Apply Changes"**.

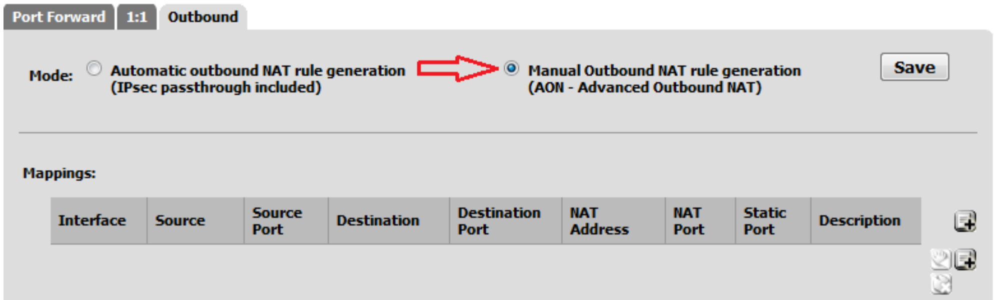


System: Advanced: System Tunables

Edit system tunable

Tunable	net.link.bridge.pfil_bridge
Description	Set to 1 to enable filtering on the bridge interface
Value	1

9. **Enable Manual outbound NAT rule generation (AON – Advanced Outbound NAT)**
    a. From the menu select **"Firewall -> NAT"** and the **"Outbound"** tab.
    b. Click **"Manual outbound NAT rule generation (AON – Advanced Outbound NAT)"** and select **"Save"**. Delete any rules that auto-populate in the mappings area.



Mode: ○ Automatic outbound NAT rule generation (IPsec passthrough included) ● Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)

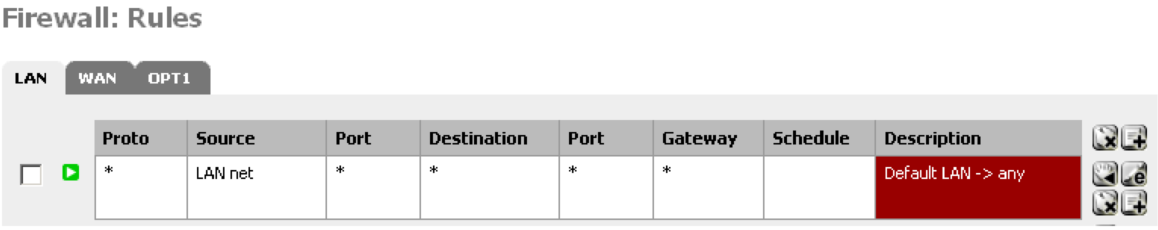
Mappings:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description

10. **Configure Hostname, Domain, DNS servers, Time zone, and NTP time server.**
    a. From the menu select **"System" -> "General Setup".**
    b. Most fields can be left default but be sure to configure your DNS server and NTP time server.

11. **Reboot pfSense Firewall**
    a. In order to fully apply all changes reboot your pfSense firewall by going to **"Diagnostics -> Reboot"**. In this menu select **"Yes"**.

12. **Restrict Access to the Management Interface**
    a. This documentation was taken from doc.pfsens.org, I found it to be very helpful. I configured the access restrictions on the LAN and WAN interfaces. http://doc.pfsense.org/index.php/Restrict_access_to_management_interface

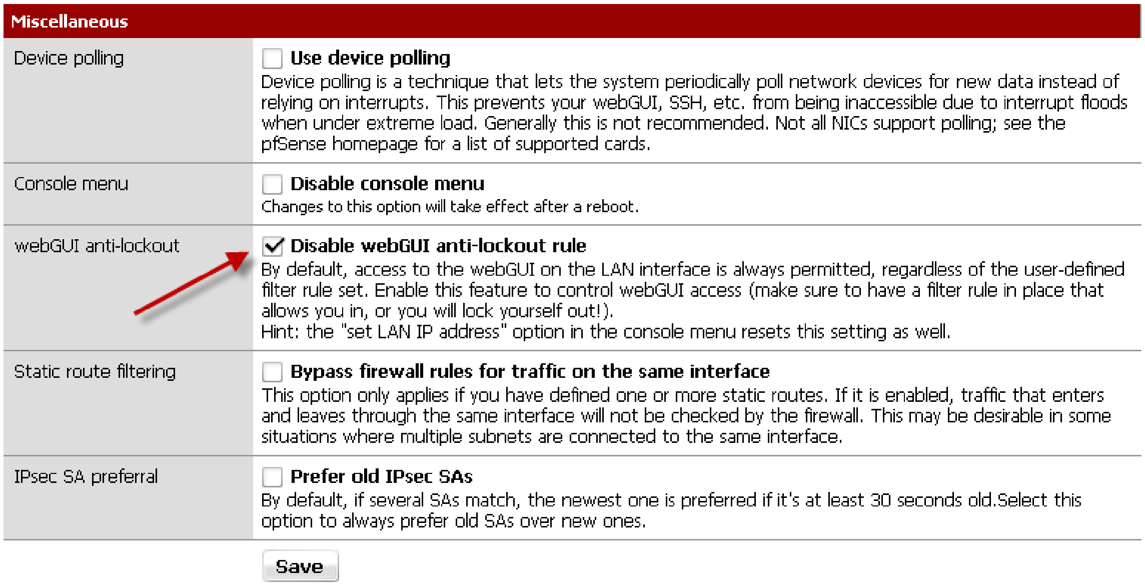


Firewall: Rules

		Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
□	▶	*	LAN net	*	*	*	*		Default LAN -> any

If you use a restrictive ruleset on your LAN, make sure it permits access to the web interface before continuing.

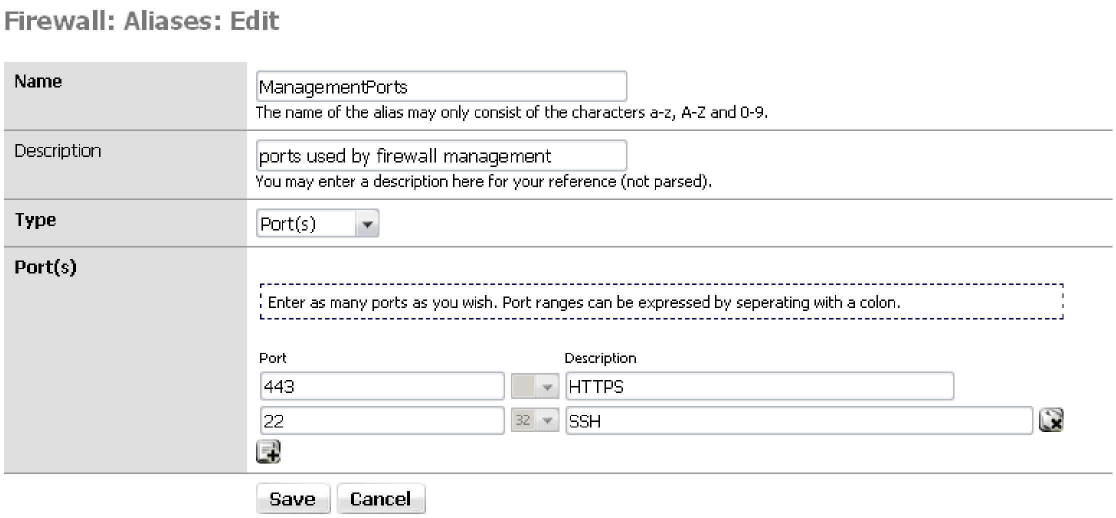
Now disable the anti-lockout rule by going to the System -> Advanced page and checking the "Disable webGUI anti-lockout rule" box. Click Save and the rule will be removed.



Miscellaneous

Device polling	□ **Use device polling** Device polling is a technique that lets the system periodically poll network devices for new data instead of relying on interrupts. This prevents your webGUI, SSH, etc. from being inaccessible due to interrupt floods when under extreme load. Generally this is not recommended. Not all NICs support polling; see the pfSense homepage for a list of supported cards.
Console menu	□ **Disable console menu** Changes to this option will take effect after a reboot.
webGUI anti-lockout	☑ **Disable webGUI anti-lockout rule** By default, access to the webGUI on the LAN interface is always permitted, regardless of the user-defined filter rule set. Enable this feature to control webGUI access (make sure to have a filter rule in place that allows you in, or you will lock yourself out!). Hint: the "set LAN IP address" option in the console menu resets this setting as well.
Static route filtering	□ **Bypass firewall rules for traffic on the same interface** This option only applies if you have defined one or more static routes. If it is enabled, traffic that enters and leaves through the same interface will not be checked by the firewall. This may be desirable in some situations where multiple subnets are connected to the same interface.
IPsec SA preferral	□ **Prefer old IPsec SAs** By default, if several SAs match, the newest one is preferred if it's at least 30 seconds old.Select this option to always prefer old SAs over new ones.

Now I suggest adding a network alias for management access, and if you use both web and SSH administration, add an alias for those ports.

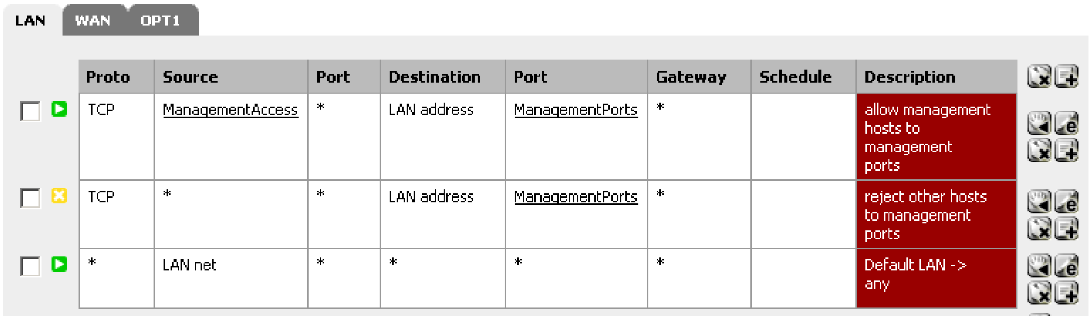


Firewall: Aliases: Edit

Name	ManagementPorts The name of the alias may only consist of the characters a-z, A-Z and 0-9.
Description	ports used by firewall management You may enter a description here for your reference (not parsed).
Type	Port(s)
Port(s)	Enter as many ports as you wish. Port ranges can be expressed by seperating with a colon.

Port		Description
443		HTTPS
22	32	SSH

Now add a firewall rule allowing the sources defined in your management alias to the destination LAN address, with the port used or alias created for those using multiple ports. Make sure this rule comes first in the list. Then add a rule based on that rule (the + next to the rule), changing action to block or reject (I prefer reject on internal networks), source to any, and destination the same. When finished your ruleset should look like the following.



		Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
☐	▶	TCP	ManagementAccess	*	LAN address	ManagementPorts	*		allow management hosts to management ports
☐	✕	TCP	*	*	LAN address	ManagementPorts	*		reject other hosts to management ports
☐	▶	*	LAN net	*	*	*	*		Default LAN -> any

Apply your changes and your management interface is now restricted to only the defined hosts.

13. Overview and Understanding of the Transparent Bridge

I use the **WAN** as the management interface because I was unable to reach anything external, obtain updates or browse packages when the **LAN** or **Bridge** was configured as the management interface.

Treat the **LAN** and **WAN** interfaces as you would a standard firewall, keep in mind that the default action in the transparent bridge is to **block** all traffic unless explicitly allowed in the firewall. You will only need to setup rules on the **LAN** and **WAN**, I have yet to touch the **Bridge**.

Generally a standard firewall will allow the **LAN** to **ANY** by default; allowing anything on the LAN outbound. In this transparent bridge scenario you **MUST** create a rule to allow your **LAN** outbound. As stated above the default behavior of the transparent bridge is to block unless explicitly allowed.

Cheers!