Setup a transparent firewall /filtering bridge with pfSense

This howto describes the way you set up a transparent firewall or fitering ridge with pfSense.

Thanks to Scott Ulrich and all the other devs for this beautiful product…

~~I use BETA2-BUGVALIDATION5 version for installation.~~
~~You can get it here: http://pfsense.com/~sullrich/BETA2-BUGVALIDATION5/~~

Neccessary things to do (depending on the platform you want to use) before you can start:

- burn the ISO to a CD and install on a pc-platform
- install the IMG on a CF-medium for a wrap-platform

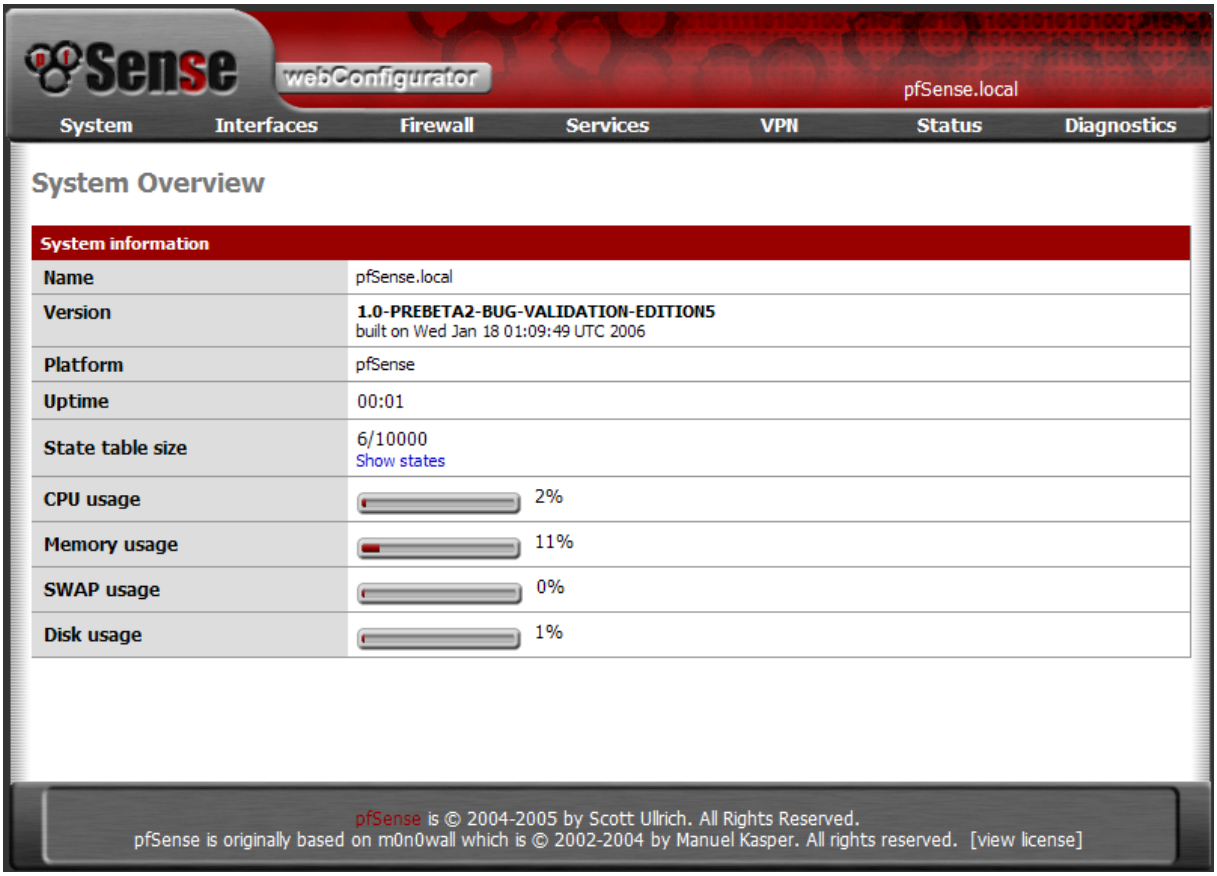
~~If you are not successful with the ISO beta2v5 use the beta1 and upgrade it with the full-update.~~
~~Sometimes the LUA-installer might die because of some curses not found…~~

Now you have a fresh pfSense install in front of you.

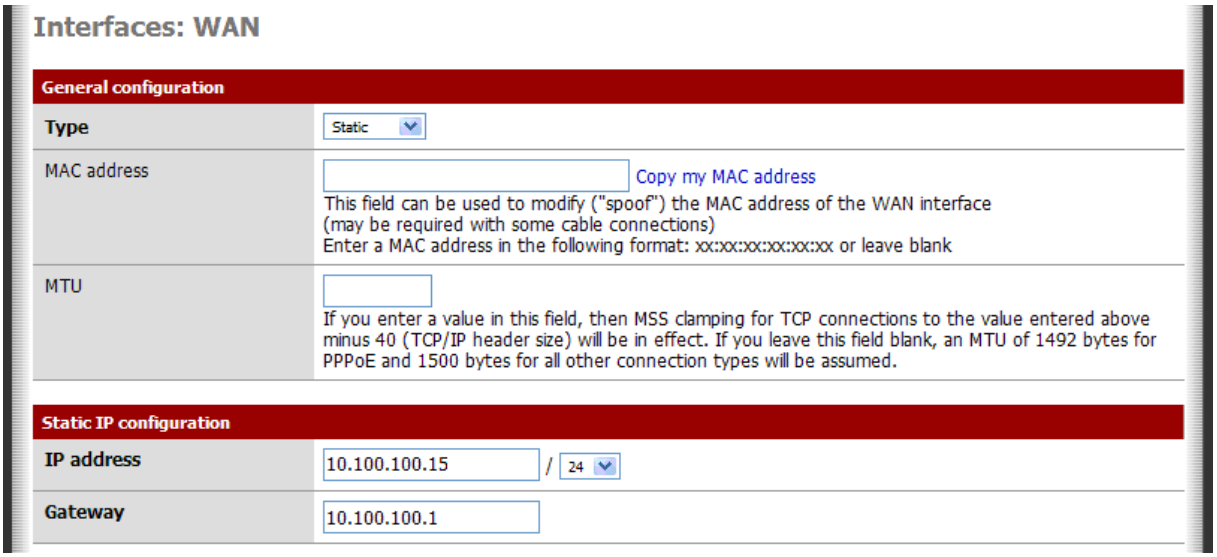
First you skip the wizard by clicking on the pfSense logo because you want to set up all parameters on your own.

Now please follow the instructions:

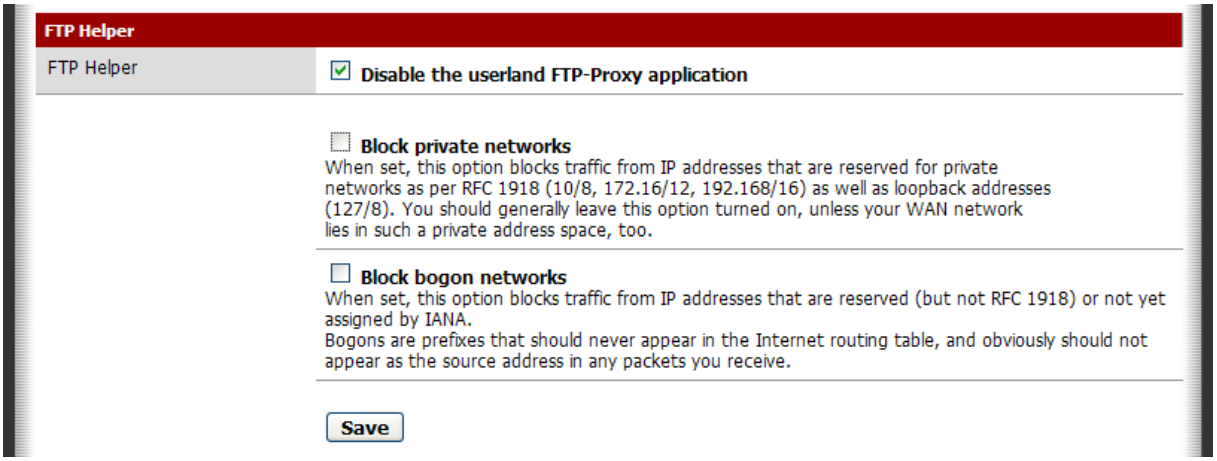
You should see this window (Status → System). This is where we start.



Now go to the Interfaces tab and chose the WAN-Interface.
Change the type to static and enter the IP you want to use as the management IP and your Internet-Gateway:



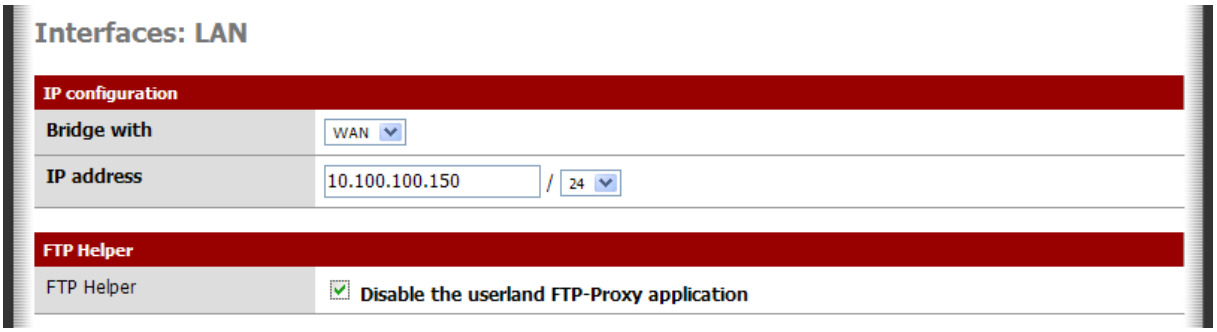
Scroll down to the *FTP-Helper settings* and disable the **Block private networks** option.



Now hit the **save** button.

After saving is complete you go to the Interfaces tab and chose the LAN-Interface.

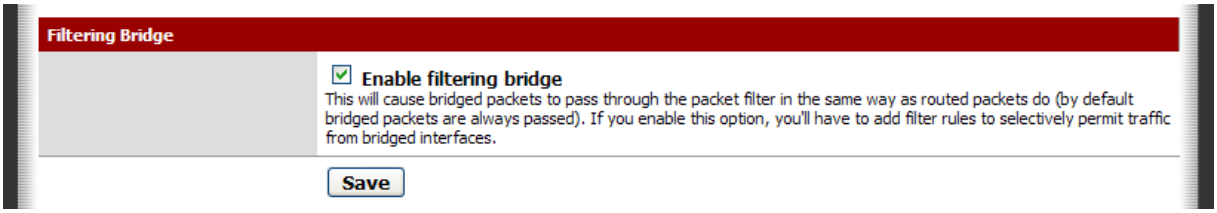
Bridge the LAN-Interface with the WAN-Interface and disable the FTP Helper.
The IP you enter here will be ignored when you activate the bridge mode.
You better should not use the same IP on both interfaces, because it can cause BSD-internal problems.
The management IP given in the WAN-settings will be assigned to the bridge interface, which will be created when activating the bridge.



Hit the **save** button.
Afterwards hit the **apply changes** button.

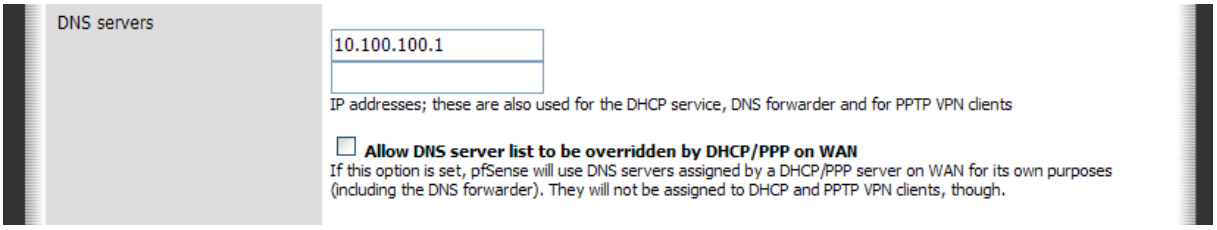
Now go to System → Advanced tab.

Enable the **filtering bridge** mode



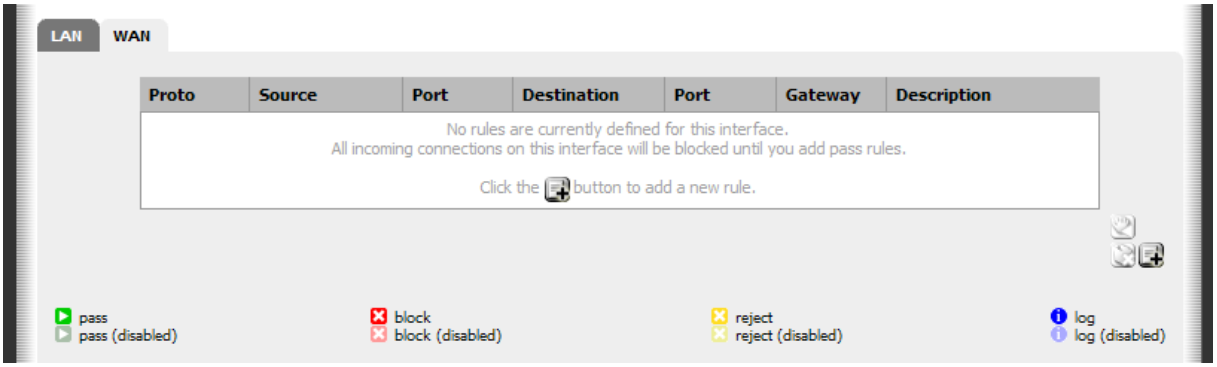
And hit the **save** button.

Now go to the System → General Setup tab and set the DNS-Server(s) and disable the DHCP override.
As a DNS server you might want to use the IP of your internal DNS server ort he IP of your internet router if it is capable of forwarding DNS queries.

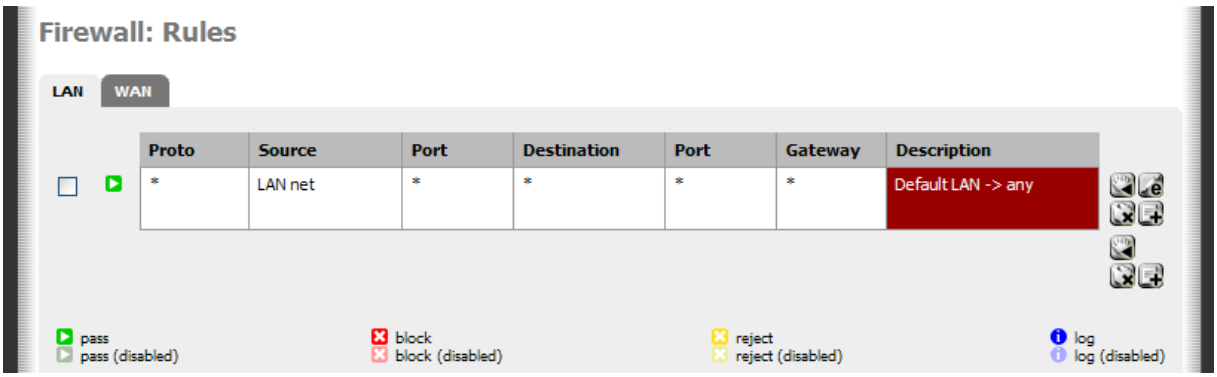


Hit the **save** button at the end of the page.

When you go to the Firewall → Rules tab now, you will first see the WAN rules.
By default no rule exists:



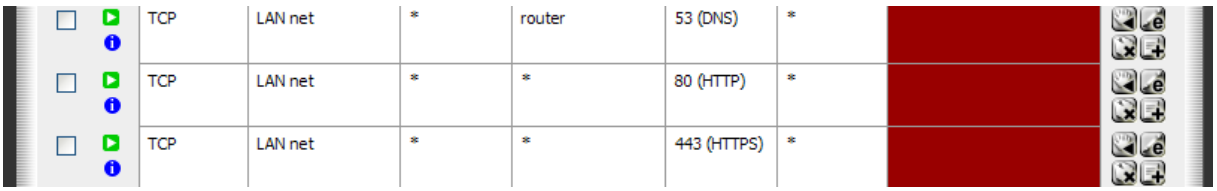
Switch to LAN now by hitting the LAN tab:



The default rule will forward all traffic from the LAN-Interface to the WAN-Interface.

For a filtering bridge you might want to disable the default rule and create some rules, which represent the ruleset you want to allow.

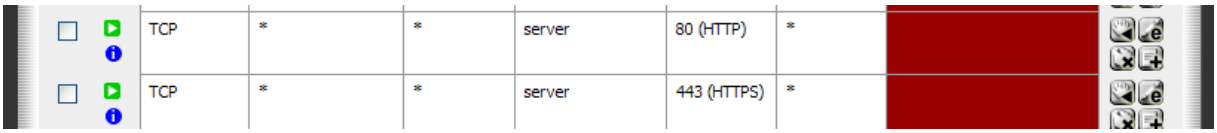
For example you have DNS, HTTP, HTTPS, SMTP, POP3 from LAN → WAN.



TCP	LAN net	*	router	53 (DNS)	*	
TCP	LAN net	*	*	80 (HTTP)	*	
TCP	LAN net	*	*	443 (HTTPS)	*	

Keep in mind that the firewall now works transparent.
This means that you also have to define what traffic is allowed to pass from the WAN-Interface.

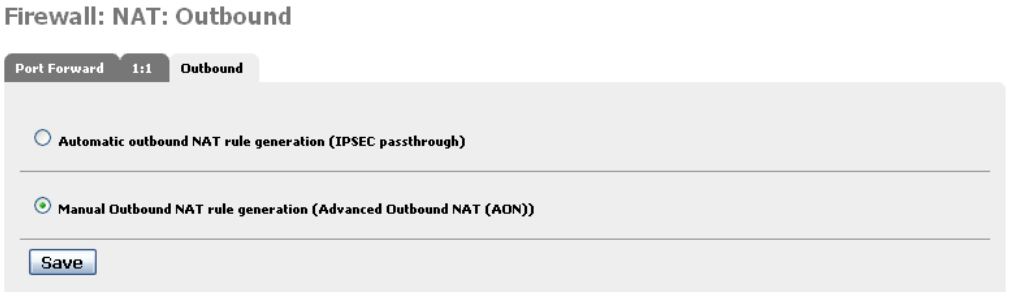
Queries coming from the WAN-Side have to be answered, ex. If you have an internal http server, you have to set up a rule for WAN → LAN with destination port 80 at the LAN side.



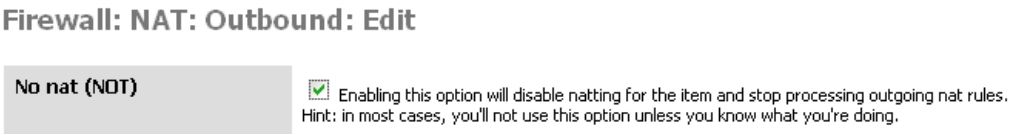
TCP	*	*	server	80 (HTTP)	*	
TCP	*	*	server	443 (HTTPS)	*	

Please also keep in mind that the option WAN address as source or destination will not be the first choice when running pfSense in transparent mode.

After that you have to switch NAT off.
Chose FIREWALL → NAT → OUTBOUND and check the advanced-outbound-nat (AON) option.



In the autocreated rule for LAN chose the no-NAT option.



Apply the settings…

There are some features that do not work with the transparent mode until now.
Perhaps this will be different in future releases.

Some features that do not work are:

- Captive portal
- Dynamic DNS (since dyndns must use the external WAN-IP)

Have a look at the following issues:

- Use FTP active mode, because FTP passive mode uses dynamic ports that you would have to open on pfSense WAN → LAN [1024 – 65535]

Troubleshooting guide:

- When traffic does not pass from LAN → WAN or vice versa, please have a look that there are not two identical IP-adresses on LAN and WAN
- Furthermore please check if the rules-direction could have changed (there were omments that rules are processed the other way round in newer Firmware-Revisions) for example LAN→ WAN ruleset sets WAN→ LAN rules…

FOR ACTUAL VERSIONS OF THIS PDF-DOCUMENT HAVE A LOOK AT HTTP://PFSENSE.TRENDCHILLER.COM