



Setup a transparent firewall /filtering bridge with pfSense

This howto describes the way you set up a transparent firewall or filtering bridge with pfSense.

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

I use ~~BETA2-BUGVALIDATIONS5~~ version for installation.

You can get it here: <http://pfsense.com/~sullrich/BETA2-BUGVALIDATIONS/>

Necessary 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.

The screenshot shows the pfSense webConfigurator interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', and 'Diagnostics'. The 'System' tab is selected, displaying the 'System Overview' page. The page features a 'System information' table with the following data:

System information	
Name	pfSense.local
Version	1.0-PREBETA2-BUG-VALIDATION-EDITIONS5 built on Wed Jan 18 01:09:49 UTC 2006
Platform	pfSense
Uptime	00:01
State table size	6/10000 Show states
CPU usage	2%
Memory usage	11%
SWAP usage	0%
Disk usage	1%

At the bottom of the page, a footer contains the following text: pfSense is © 2004-2005 by Scott Ulrich. All Rights Reserved. pfSense is originally based on m0n0wall which is © 2002-2004 by Manuel Kasper. All rights reserved. [view license]

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:

Interfaces: WAN

General configuration	
Type	Static
MAC address	<input type="text"/> Copy my MAC address This field can be used to modify ("spoof") the MAC address of the WAN 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	<input type="text"/> 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. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
Static IP configuration	
IP address	<input type="text" value="10.100.100.15"/> / <input type="text" value="24"/>
Gateway	<input type="text" value="10.100.100.1"/>

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

FTP Helper

FTP Helper	<input checked="" type="checkbox"/> Disable the userland FTP-Proxy application
	<input type="checkbox"/> Block private networks When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.
	<input type="checkbox"/> Block bogon networks When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.
<input type="button" value="Save"/>	

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.

Interfaces: LAN

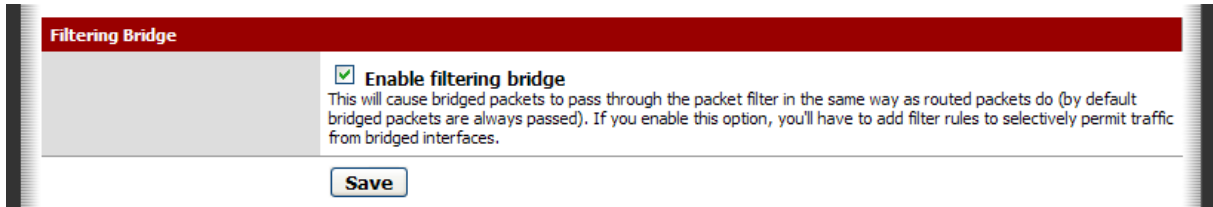
IP configuration	
Bridge with	WAN
IP address	<input type="text" value="10.100.100.150"/> / <input type="text" value="24"/>
FTP Helper	
FTP Helper	<input checked="" type="checkbox"/> Disable the userland FTP-Proxy application

Hit the **save** button.

Afterwards hit the **apply changes** button.

Now go to System → Advanced tab.

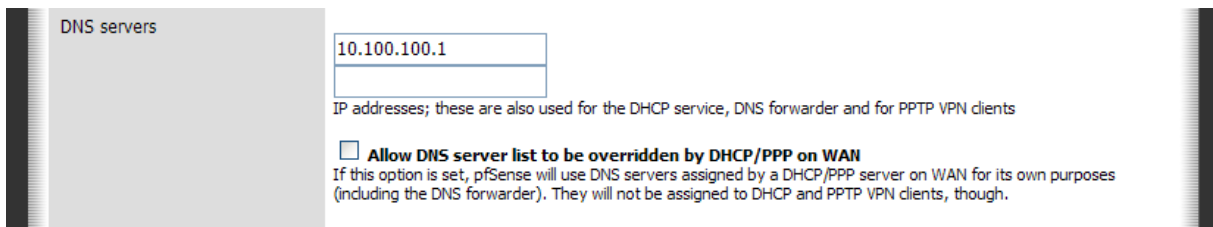
Enable the **filtering bridge** mode



And hit the **save** button.

Now go to the System → General Setup tab and set the DNS-Server(s) and disable the DHCP override.

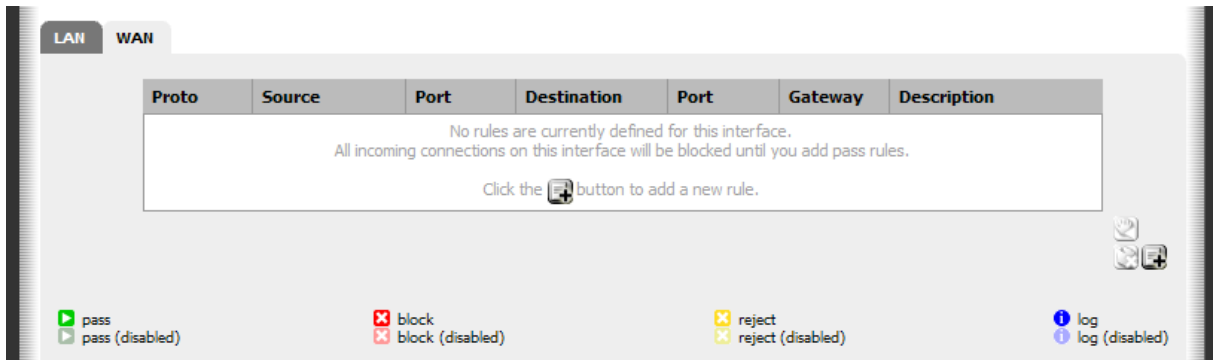
As a DNS server you might want to use the IP of your internal DNS server or the IP of your internet router if it is capable of forwarding DNS queries.



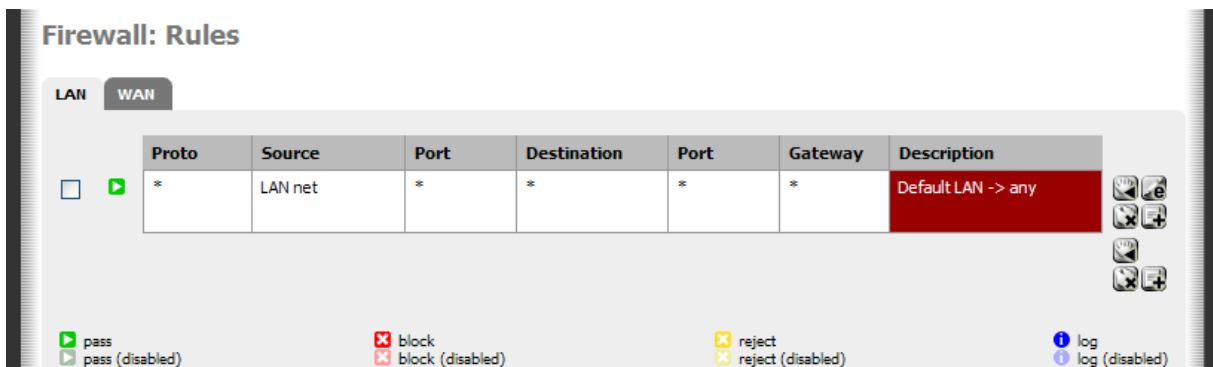
Hit the **save** button at the end of the page.

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.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	TCP	LAN net	*	router	53 (DNS)	*	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	TCP	LAN net	*	*	80 (HTTP)	*	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	TCP	*	*	server	80 (HTTP)	*	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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.

Firewall: NAT: Outbound

Port Forward 1:1 Outbound

Automatic outbound NAT rule generation (IPSEC passthrough)

Manual Outbound NAT rule generation (Advanced Outbound NAT (AON))

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

Firewall: NAT: Outbound: Edit

No nat (NOT) Enabling this option will disable natting for the item and stop processing outgoing nat rules.
Hint: in most cases, you'll not use this option unless you know what you're doing.

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](http://pfsense.trendchiller.com)