PFSENSE
Load Balance with Fail Over
From Version Beta3

Following are the Installation instructions of PFSense beginning at first Login to setup Load Balance and Fail over procedures for outbound Internet traffic. Outbound Terminology means LAN users Internet requests. It is advisable to check for any current updates and apply them prior to configuring PFSense. It is also advisable to configure PFSense manually for each installation; it is not recommended that you import a previous configuration file. This configuration manual also assumes that you understand how to install PFSense and that you PC Hardware is configured with 3 or more Network Adaptors. This tutorial covers a basic Load Balance and Fail over installation only and does NOT cover Hardened Firewall procedures.

What hardware will I need?

PFSense Hardware compatibility can be found at the following link. To load balance Internet connections you will need a minimum of PC with a
133MHz CPU but 400MHz CPU is recommended with
Minimum of 128MB RAM and a
1GB Hard Drive
3 Network Interface Adaptors
2 ADSL Ethernet Routers
2 Static IP Addresses from your ISP
Most Likely 2 ADSL Accounts
2 Telephone Lines with ADSL enabled

http://www.pfsense.com/index.php?id=37

The PFSense Firewall PC specifications that this document was create on uses the following

Intel P4 2GHz CPU
1GB pc2700 RAM (2 x 512MB Dual Channel)
40GB IDE ATA100 Harddrive
4 Netgear GA311 Gigabit Network Interface Adaptors with the Realtek 81695 chipset
2 DLInk DSL-502T ADSL Routers
2 Static IP Addresses from ISP
2 ADSL Accounts
2 Telephone lines ADSL enabled

Alternative PFSense compatible Hardware configurations can be found at;

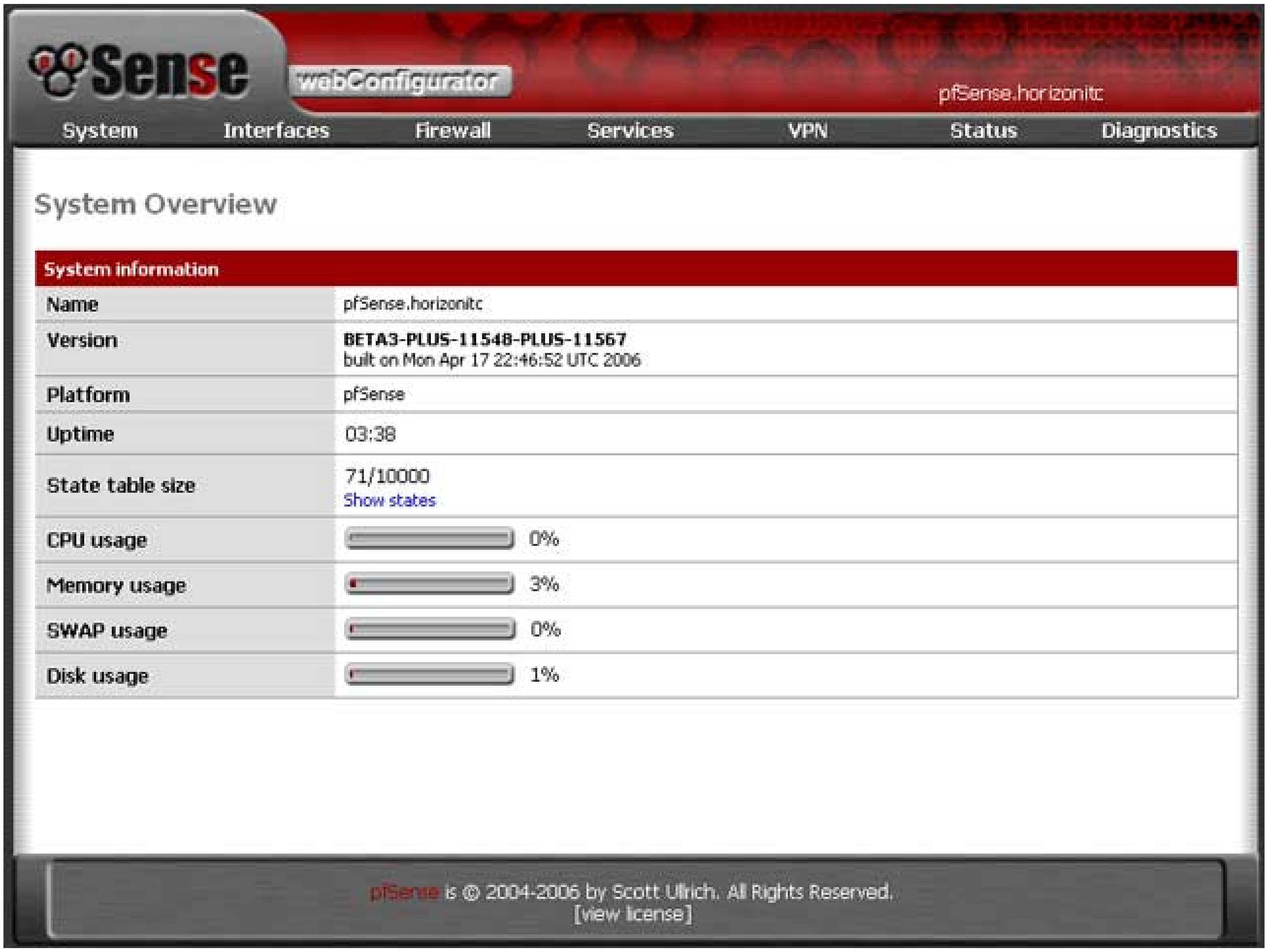
http://www.pfsense.com/index.php?id=40

Plan your PFSense Network Configuration Addresses prior to setup, it makes it easier during the setup process. Ensure that you DO NOT use conflicting IP Address ranges and Subnets. LAN and WAN and OPT addresses can not begin with the same IP range. You will ADSL Routers to suit the Static IP Address Range that you have chosen for your Gatway's for both WAN and OPT Interfaces.

If you require instructions on configuring an additional LAN or DMZ interfaces, please visit the PFSense website for Tutorials and the Support Forum for additional assistance.

FIRST LOGIN

The first Login to PFSense using your web browser and navigate to http://192.168.1.1 and use the Username: ***admin*** and the Password: ***pfsense*** to administer your PFSense firewall. You will be greeted by PFSense System Overview page which will look like:



System Overview

System information	
Name	pfSense.horizonitc
Version	**BETA3-PLUS-11548-PLUS-11567** built on Mon Apr 17 22:46:52 UTC 2006
Platform	pfSense
Uptime	03:38
State table size	71/10000 Show states
CPU usage	0%
Memory usage	3%
SWAP usage	0%
Disk usage	1%

pfSense is © 2004-2006 by Scott Ullrich. All Rights Reserved.
[view license]

PLANNED CONFIGURATION

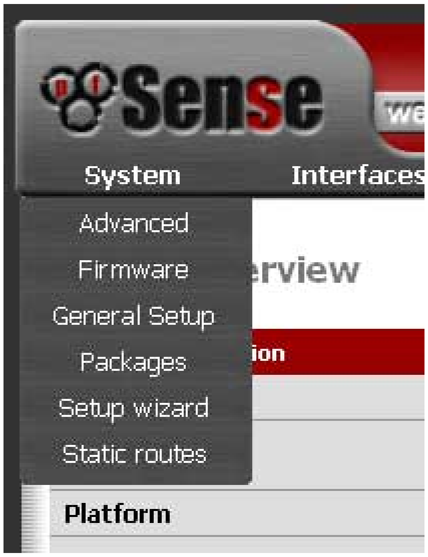
LAN IP Address:	192.168.1.1

WAN IP Address:	190.165.30.30
WAN IP Gateway:	190.165.30.2
WAN Router IP:	190.165.30.2
Internet Static IP:	ISP Assigned

OPT1 IP Address:	189.165.20.20
OPT1 IP Gateway:	189.165.20.2
OPT1 Router IP:	189.165.20.2
Internet Static IP:	ISP Assigned

STEP 2

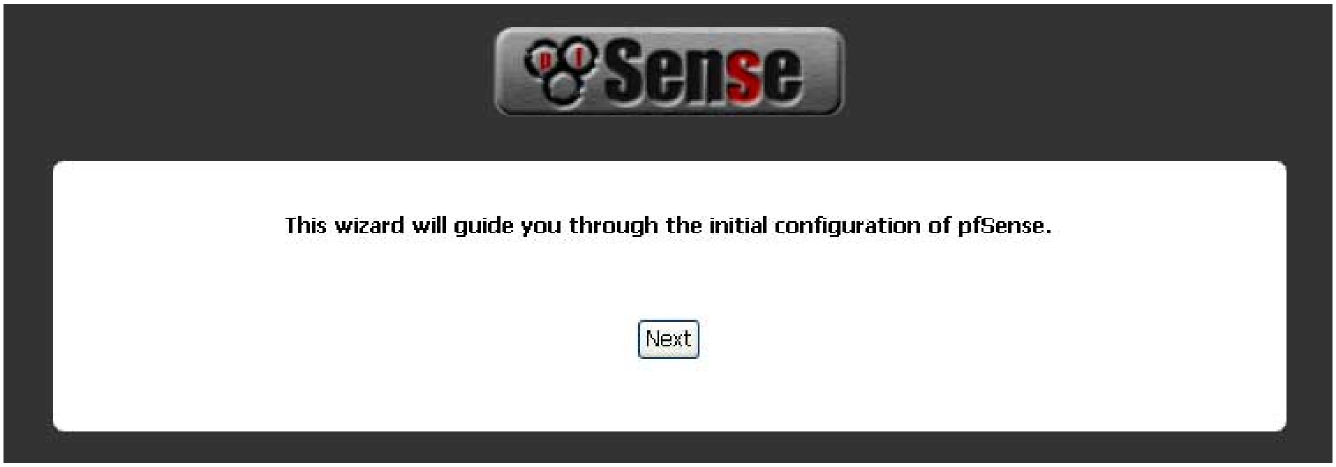
Selecting from the System Menu, use either the Setup Wizard or General Setup to manually setup your PFSense Firewall.



STEP 3

Using the Setup Wizard, it will lead you through the setup process to customize your PFSense Firewall to your global location time zone, the DNS server IP addresses of your ISP, set your Admin password, your LAN IP (Recommend leaving set as default) and then to the WAN Interface.

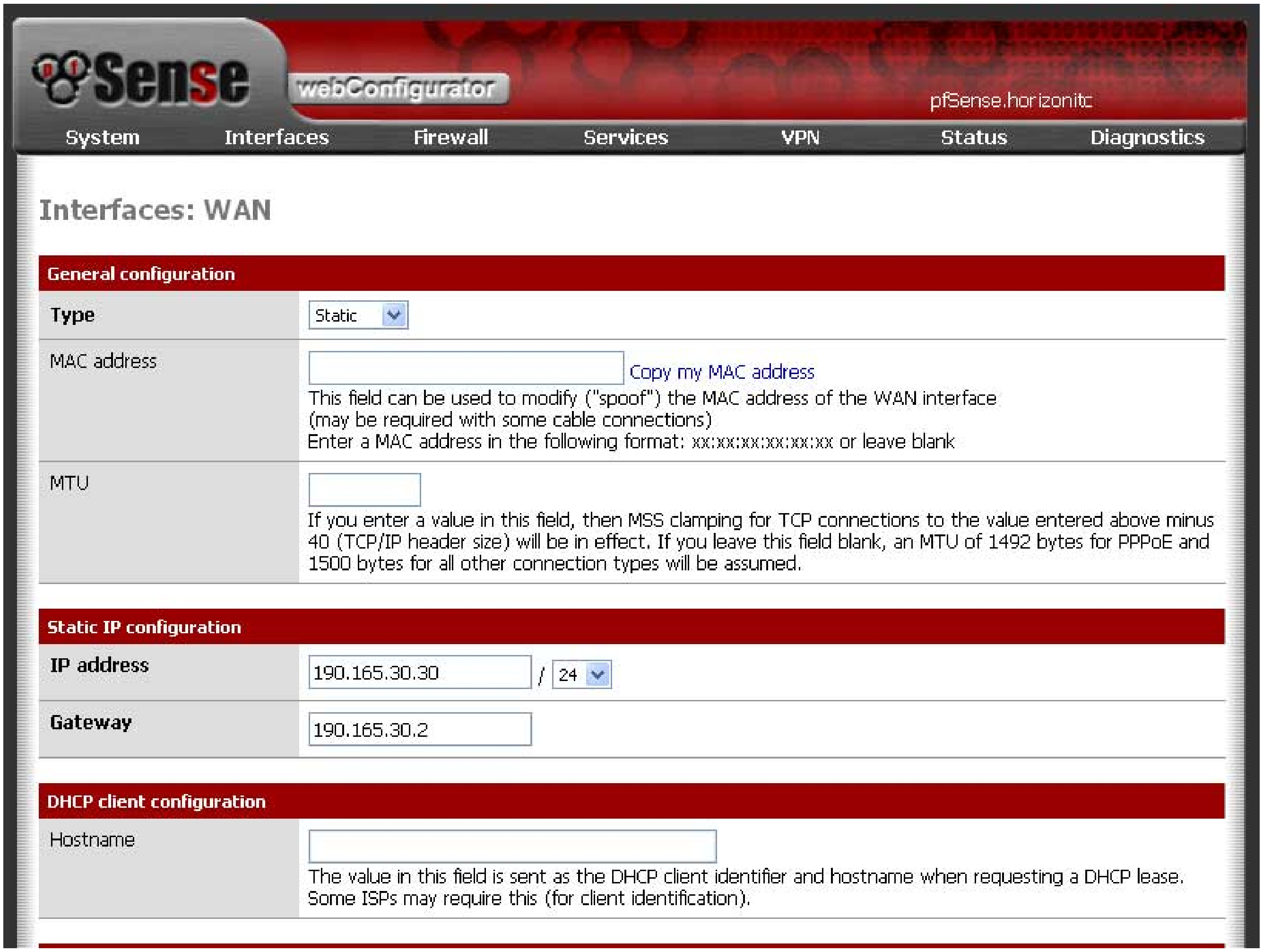
It is advisable to plan ahead what IP address ranges you are going to use.



This wizard will guide you through the initial configuration of pfSense.

STEP 4

Setting up your WAN Interface for Load Balance, you will need to set a static IP address for it, not using PPPOE or PPPOA as are options. Below is an example of this static IP configuration and static gateway. When this is done, you may save this WAN configuration. If you fail to have internet access due to your IP address range, you may need to unblock private networks to allow traffic to pass through.



Interfaces: WAN

General configuration

Type	Static
MAC address	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	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

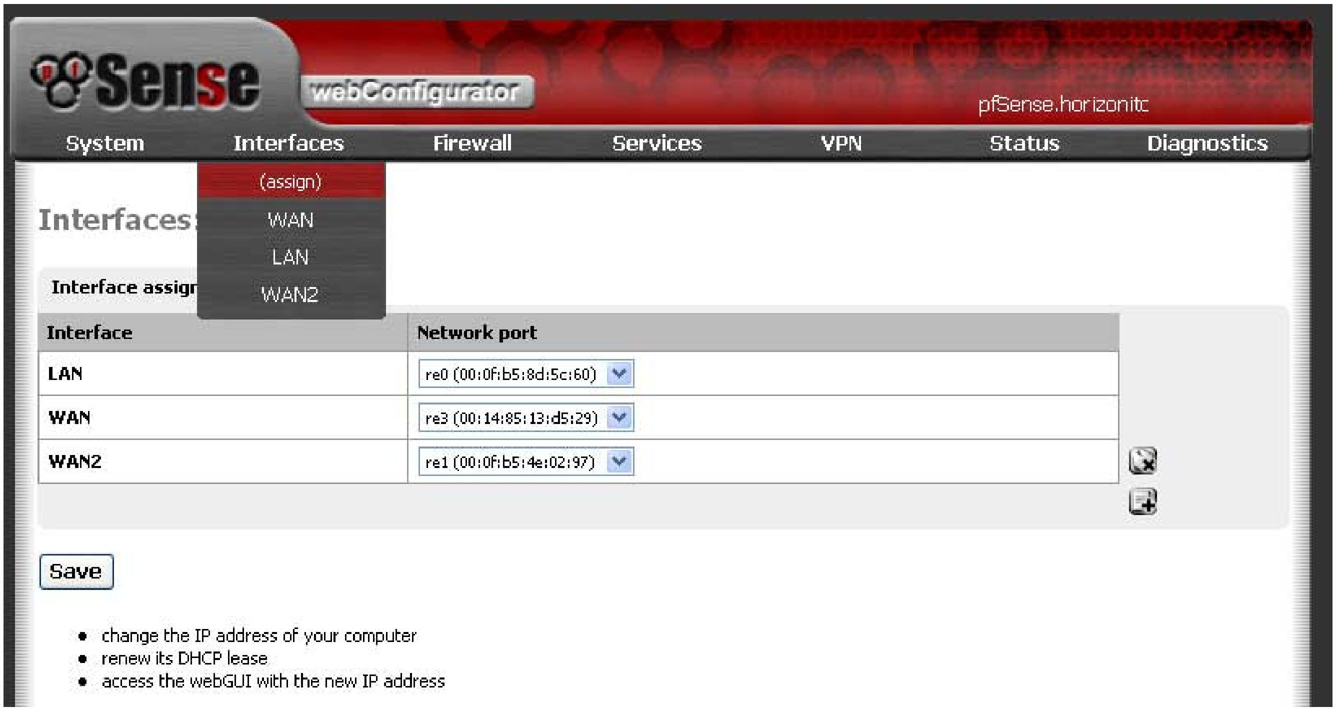
IP address	190.165.30.30 / 24
Gateway	190.165.30.2

DHCP client configuration

Hostname	The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

STEP 5

If you have not selected the your OPT interface for your second Internet connection during your installation, you can select it from the Interface Assign Menu. Your OPT Interface can then be configured at OPT1 on the Interface. Below you will WAN2 this is OPT1. OPT1 can have a description that is easier to remember, this can be of your choice. Save your selection.



Interfaces:

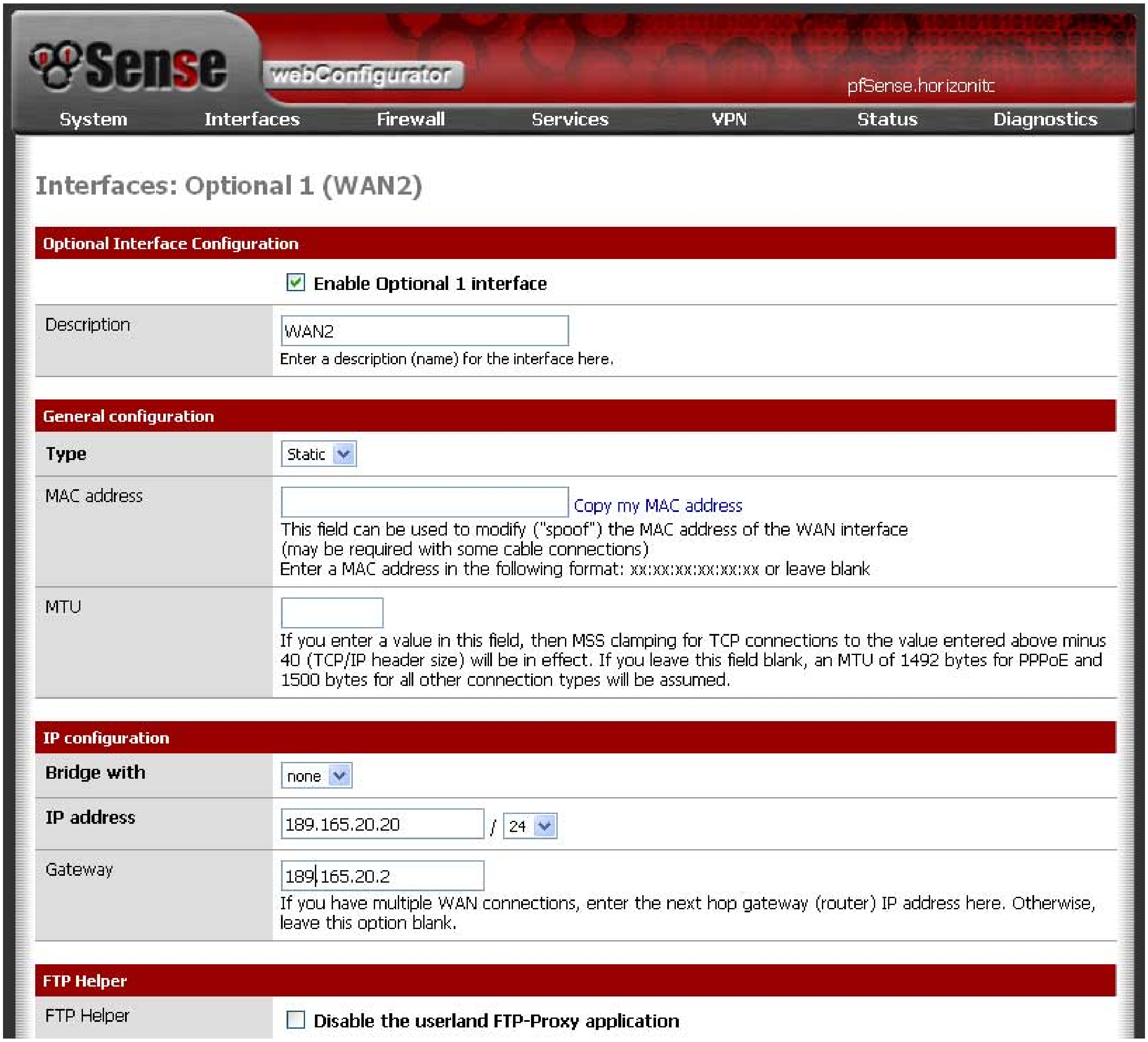
Interface assign

Interface	Network port
LAN	re0 (00:0f:b5:8d:5c:60)
WAN	re3 (00:14:85:13:d5:29)
WAN2	re1 (00:0f:b5:4e:02:97)

- change the IP address of your computer
- renew its DHCP lease
- access the webGUI with the new IP address

STEP 6

OPT1 Interface configuration uses static IP address also. OPT Interfaces do not currently support PPPOE or PPPOA. The best Alternative is to manually set static IP addresses then click the save button.



Interfaces: Optional 1 (WAN2)

Optional Interface Configuration

	☑ Enable Optional 1 interface
Description	WAN2 Enter a description (name) for the interface here.

General configuration

Type	Static
MAC address	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	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.

IP configuration

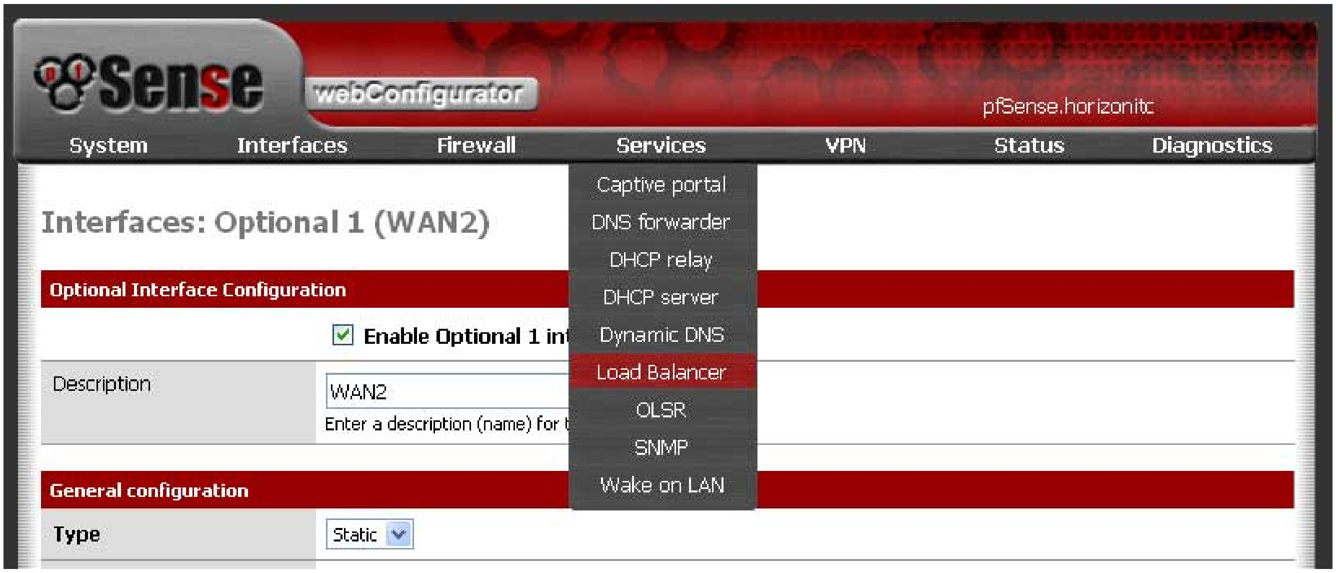
Bridge with	none
IP address	189.165.20.20 / 24
Gateway	189.165.20.2 If you have multiple WAN connections, enter the next hop gateway (router) IP address here. Otherwise, leave this option blank.

FTP Helper

FTP Helper	☐ Disable the userland FTP-Proxy application

STEP 7

Setting up the Load Balance Pool, from the services menu select Load Balancer.



Interfaces: Optional 1 (WAN2)

Optional Interface Configuration

☑ Enable Optional 1 int

Description: WAN2

Enter a description (name) for t

General configuration

Type: Static

STEP 8

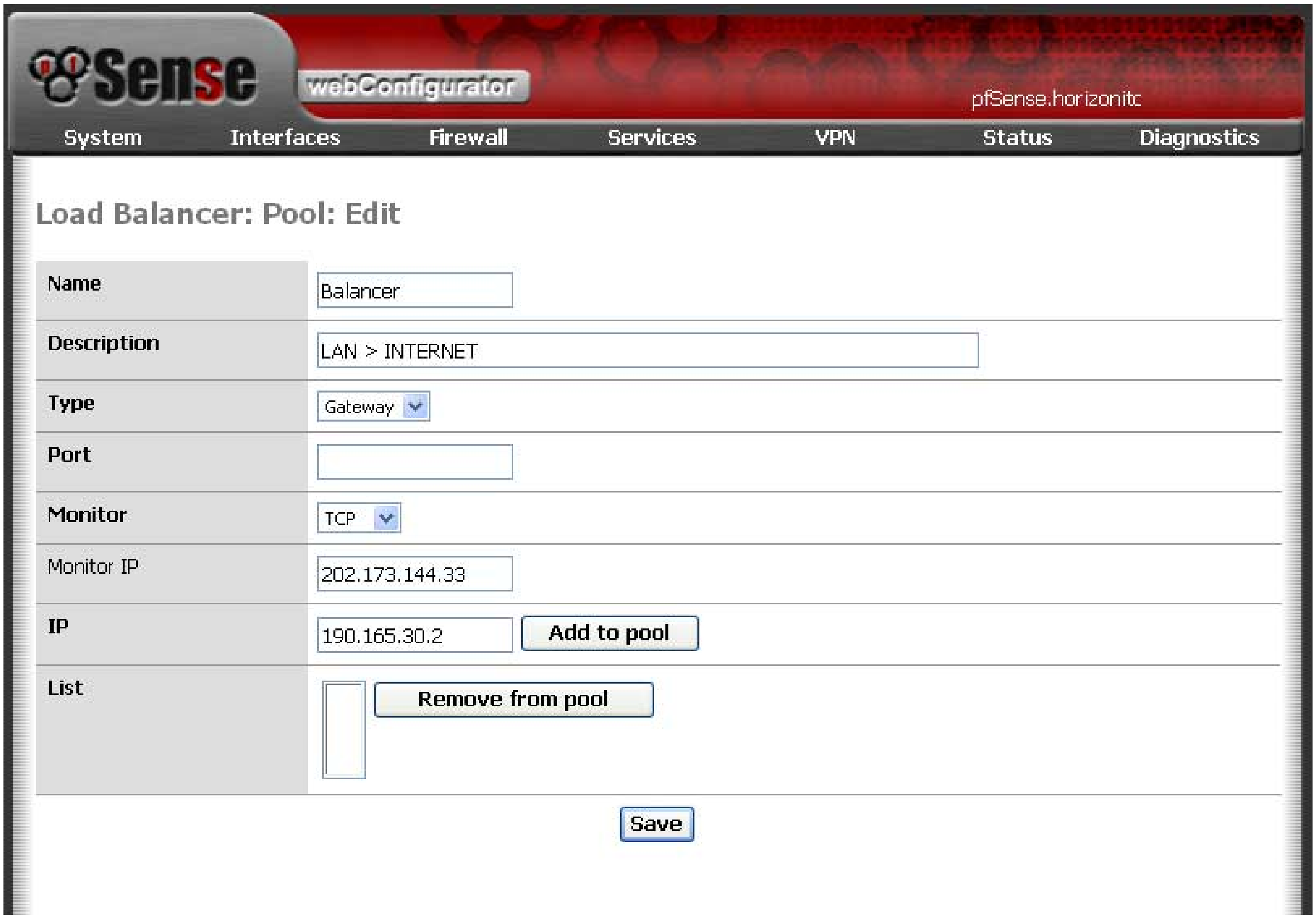
Create your Load Balance Pool by selecting the ⊞ symbol. It will bring up the window below. As an example I have created one IP Address ready to add to the Pool. Select Add to Pool when your have chosen either your WAN gateway IP or your OPT Gateway.

*** ***IMPORTANT**** Ensure that your WAN and OPT Monitor IP Addresses are not the same IP. It is advisable to use an IP address that is associated with your ISP for that Interface. EG: *WAN ISP is ABC then use their Gateway for the monitor IP, OPT ISP is XYZ then use that gateway for that monitor IP.*

EXAMPLE:

```
                    WAN 190.165.30.30 ====== [Router Static IP] ======{Internet Monitor IP 202.173.144.33}
                             ||
LAN192.168.1.1========[PFSense]LoadBalance
                             ||
                   OPT1 189.165.20.20 ====== [Router Static IP] ======{Internet Monitor IP 202.173.144.81}
```

When you have finished creating your balance pool click the save button.



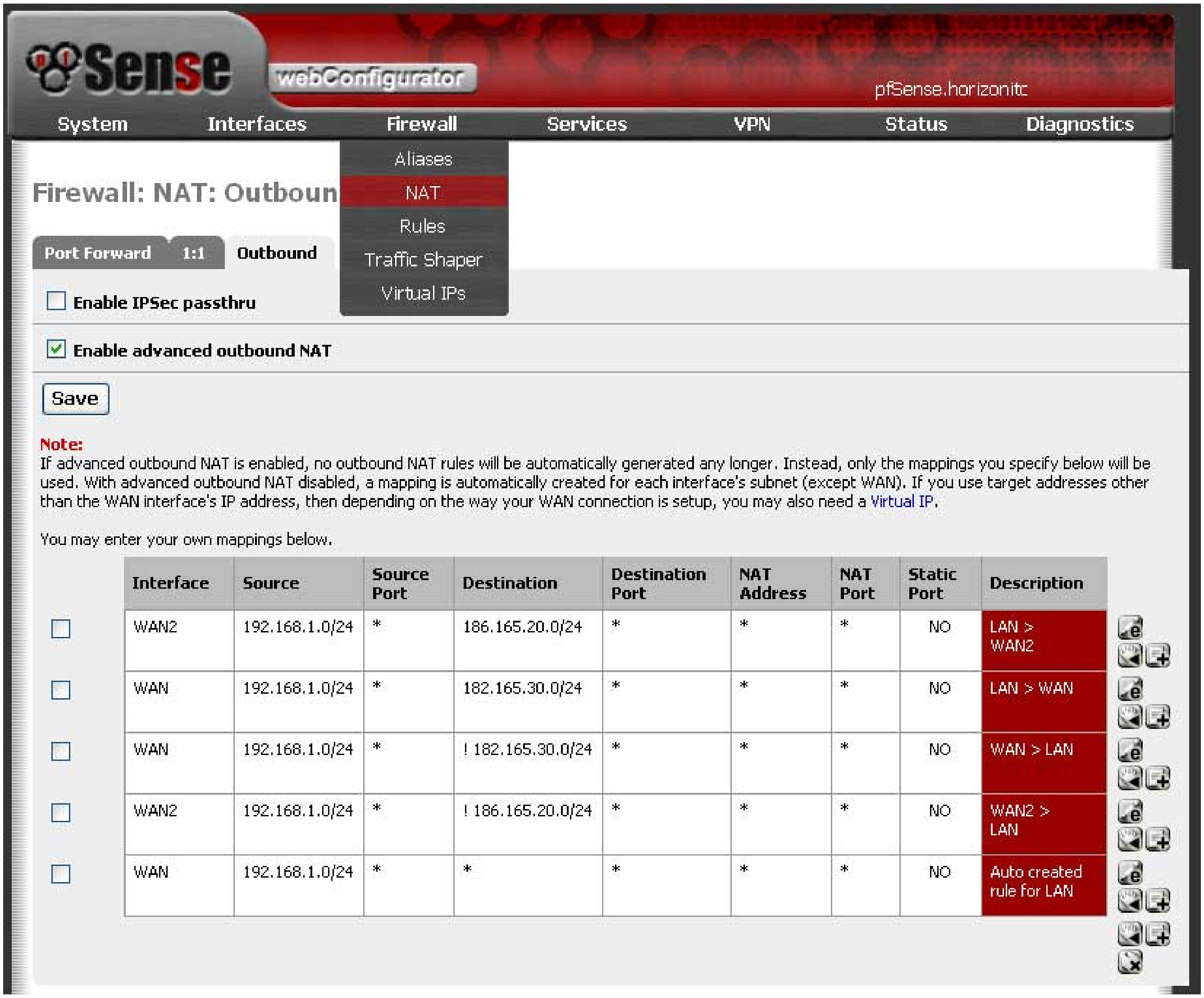
Load Balancer: Pool: Edit

Name	Balancer
Description	LAN > INTERNET
Type	Gateway
Port	
Monitor	TCP
Monitor IP	202.173.144.33
IP	190.165.30.2
List	

STEP 9

Next step will be to setup the NAT part of the firewall. In my selection I have NAT for both Inbound and Outbound for each interface, WAN and OPT1 (Alias WAN2). By default Advanced outbound NAT is not selected, but are automatically generated. You will need to enable the advanced option and SAVE it. Please note that the IP address range in the NAT below is required to be from your IP Address Range. IP Address below are and example.

After Advanced NAT has been enabled, you may then create each NAT rule.



Firewall: NAT: Outboun

□ Enable IPSec passthru

☑ Enable advanced outbound NAT

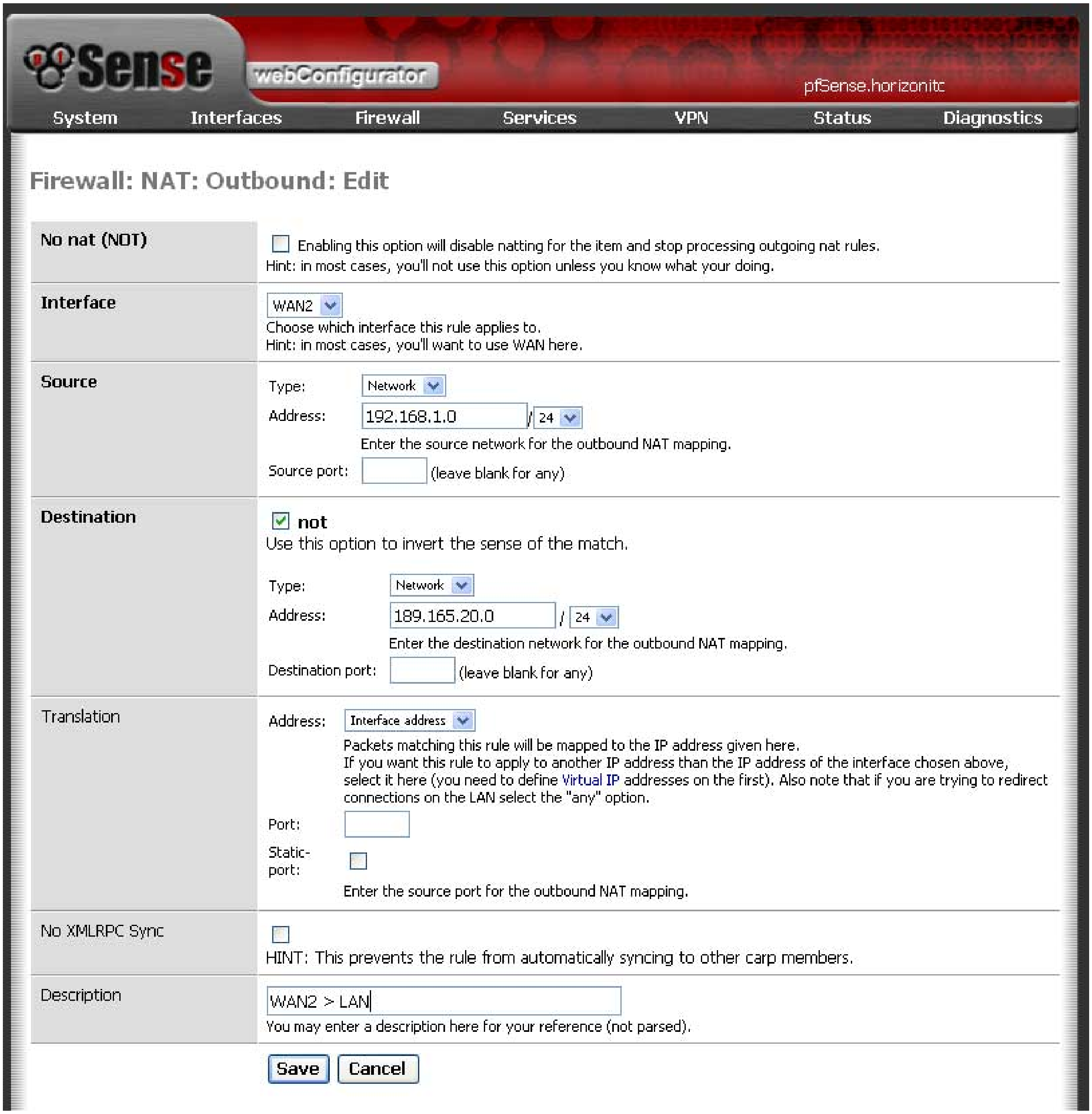
Note:
If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated any longer. Instead, only the mappings you specify below will be used. With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN). If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need a Virtual IP.

You may enter your own mappings below.

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
□	WAN2	192.168.1.0/24	*	186.165.20.0/24	*	*	*	NO	LAN > WAN2
□	WAN	192.168.1.0/24	*	182.165.30.0/24	*	*	*	NO	LAN > WAN
□	WAN	192.168.1.0/24	*	! 182.165.30.0/24	*	*	*	NO	WAN > LAN
□	WAN2	192.168.1.0/24	*	! 186.165.20.0/24	*	*	*	NO	WAN2 > LAN
□	WAN	192.168.1.0/24	*	*	*	*	*	NO	Auto created rule for LAN

STEP 10

A Blank form for creating NAT rules below demonstrates allowing NAT from OPT1 to LAN. Create these NAT Rules for both WAN and OPT1 Interfaces. Also order placing these NAT rules will have an affect on how your PFSense firewall behaves.



Firewall: NAT: Outbound: Edit

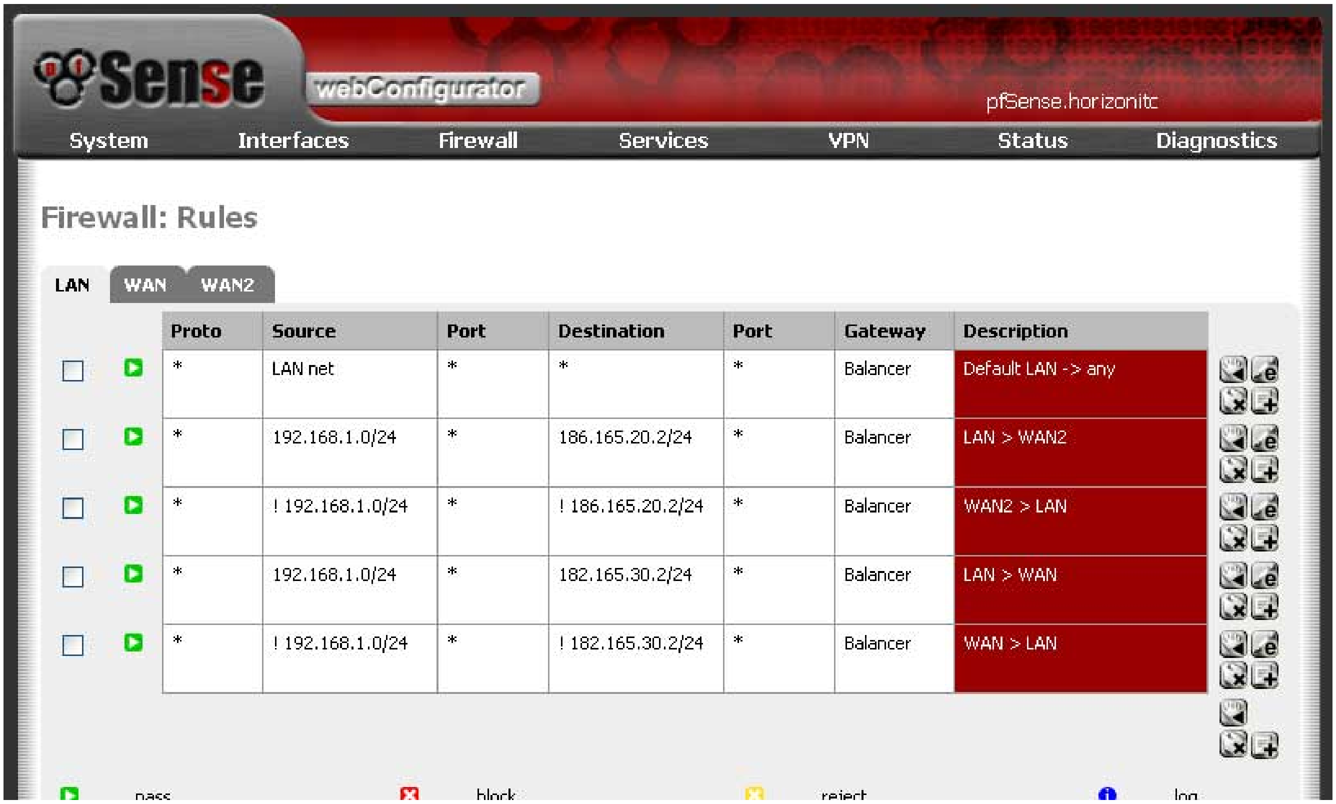
No nat (NOT)	□ Enabling this option will disable natting for the item and stop processing outgoing nat rules. Hint: in most cases, you'll not use this option unless you know what your doing.
Interface	WAN2 Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Source	Type: Network Address: 192.168.1.0 / 24 Enter the source network for the outbound NAT mapping. Source port: (leave blank for any)
Destination	☑ **not** Use this option to invert the sense of the match. Type: Network Address: 189.165.20.0 / 24 Enter the destination network for the outbound NAT mapping. Destination port: (leave blank for any)
Translation	Address: Interface address Packets matching this rule will be mapped to the IP address given here. If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. Port: Static-port: □ Enter the source port for the outbound NAT mapping.
No XMLRPC Sync	□ HINT: This prevents the rule from automatically syncing to other carp members.
Description	WAN2 > LAN You may enter a description here for your reference (not parsed).

STEP 11

When creating firewall rules for each Interface, you will have to place rules that require a higher priority first. This due to which ever rule is first in the List will take precedence above the others. So if you want a Particular protocol to take a set path, then these must be in a higher priority.

You will have to create rules for each Interface for both Incoming and outgoing. Below are some examples of rules set on another PFSense machine.

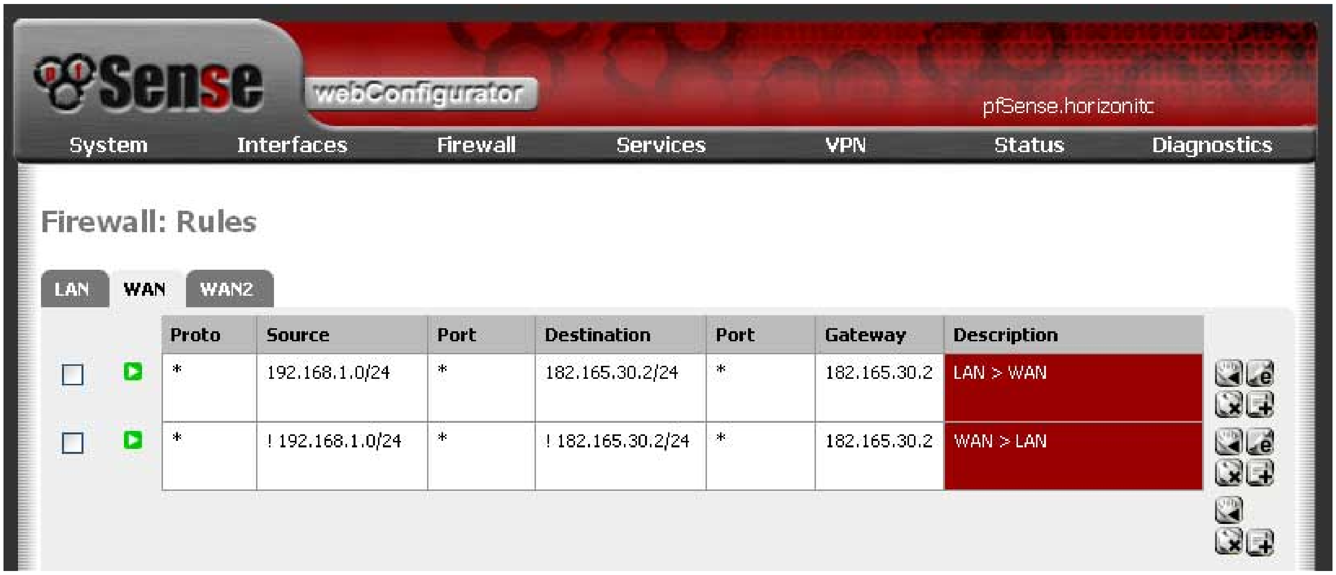
LAN RULES



Firewall: Rules

		Proto	Source	Port	Destination	Port	Gateway	Description
☐	▶	*	LAN net	*	*	*	Balancer	Default LAN -> any
☐	▶	*	192.168.1.0/24	*	186.165.20.2/24	*	Balancer	LAN > WAN2
☐	▶	*	! 192.168.1.0/24	*	! 186.165.20.2/24	*	Balancer	WAN2 > LAN
☐	▶	*	192.168.1.0/24	*	182.165.30.2/24	*	Balancer	LAN > WAN
☐	▶	*	! 192.168.1.0/24	*	! 182.165.30.2/24	*	Balancer	WAN > LAN

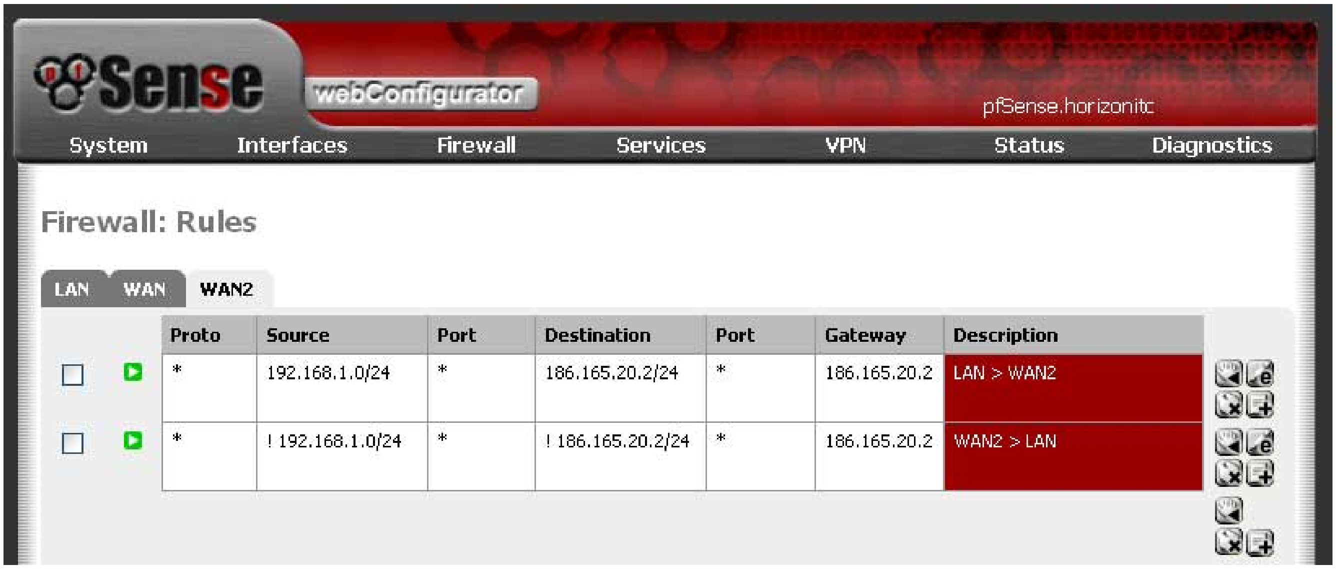
WAN RULES



Firewall: Rules

		Proto	Source	Port	Destination	Port	Gateway	Description
□	▶	*	192.168.1.0/24	*	182.165.30.2/24	*	182.165.30.2	LAN > WAN
□	▶	*	! 192.168.1.0/24	*	! 182.165.30.2/24	*	182.165.30.2	WAN > LAN

OPT1 RULES



Firewall: Rules

		Proto	Source	Port	Destination	Port	Gateway	Description
□	▶	*	192.168.1.0/24	*	186.165.20.2/24	*	186.165.20.2	LAN > WAN2
□	▶	*	! 192.168.1.0/24	*	! 186.165.20.2/24	*	186.165.20.2	WAN2 > LAN

CREATING RULES

When creating rules for the LAN interface for Load Balancing ensure that you select the Load Balance Pool. If you require a specified path for a given protocol or port, then specify that Port, Protocol and destination and selected gateway and place a higher priority to that rule.

When creating Rules for WAN and OPT Interfaces, ensure that when you select the Gateway, ensure that it is the gateway for that Interface as specified on the WAN and OPT1 Interface pages.

You will also have to create a Rule to "Invert the sense of the match", which means if the default is to go to the internet, then to invert means to bring back in to the LAN.

EG: WAN IP Address: 190.165.30.30
WAN IP Gateway: 190.165.30.2

STEP 12

Router Setup When you setup the Ethernet port on the Router allocates the LAN side (not Internet side) the IP Address of either the WAN Gateway IP or the OPT1 Gateway IP. Ensure that you enable NAT, this will assist PFSense gain the DNS information that is required for Internet access.

If you are unable to gain access to your Router through PFSense itself, then it is probable that you will have to connect it directly to a LAN client and configure it prior to connecting to PFSense Firewall.

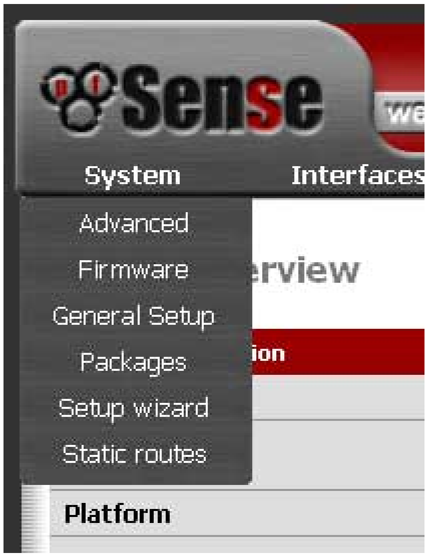
Router Security To assist in securing your PFSense firewall, it may be a desired feature that each Router does not respond to "Denial of Service Attacks", "Flood Pings", External Pings" and other undesired Internet Based attacks. If you're Router have these Firewall features it may be advisable to utilize these security features. Please refer to your Router Manufacturer Users manual.

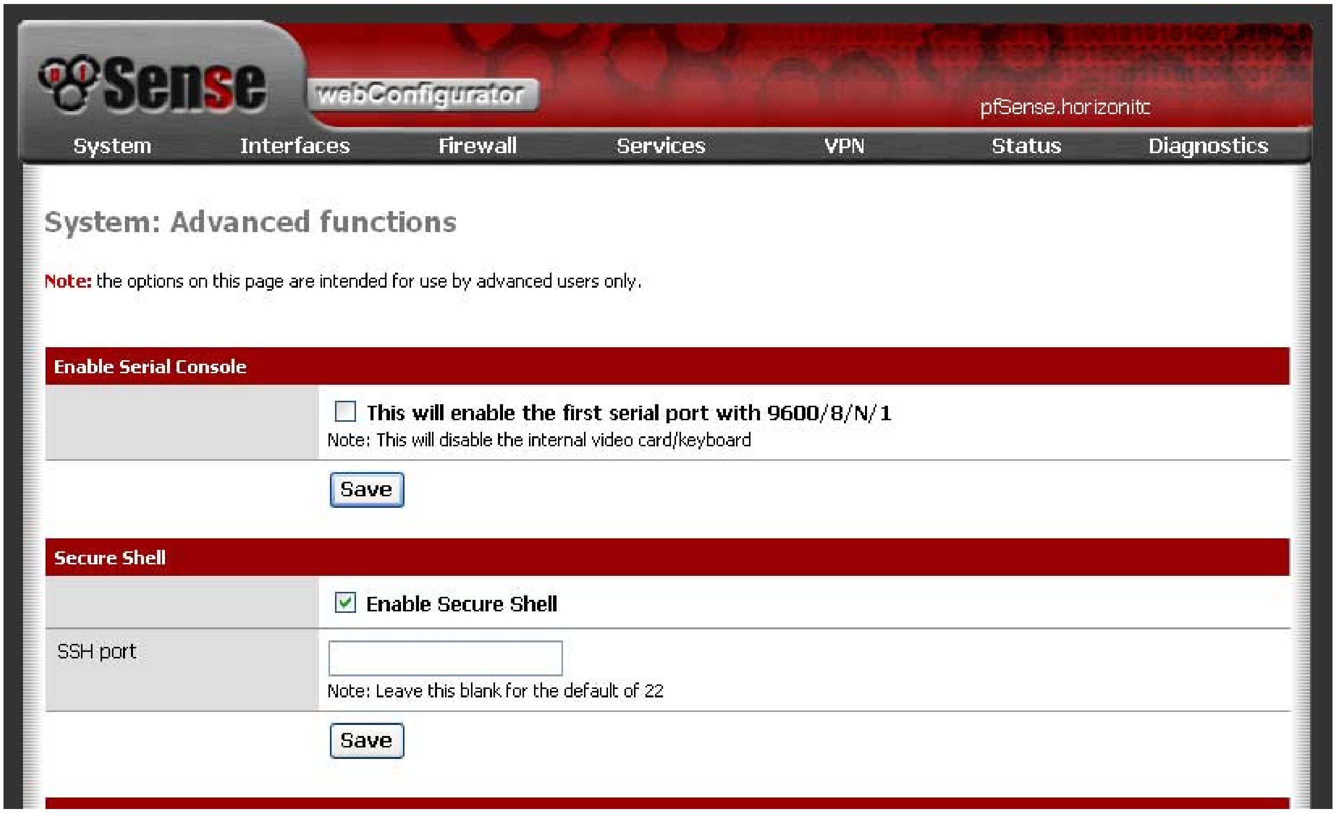
DMZ Access Enabling Router Security Firewall and blocking or dropping External Requests, may prevent you from having DMZ or Remote Access to Servers or PFSense itself. If remote access is required and you desire to tighten up the Security on your PFSense Firewall, use the following. This will take time by Closing all access and then slowly easing security until you have a secure Firewall but have the desired access control.

Testing Firewall Security To test firewall security, Internet Based Security companies have Website features that will test Firewalls, Routers and Clients from a remote location. This is done by you inviting the company to test your security which also produces a report that may assist you in your Firewall Security. There are a number of User Pay and Subscription options available. For a quick security check that is FREE, try using the Gibson Research Centre Website "ShieldsUP Test" on http://www.grc.com

Finally When you have configured all your Rules and NAT and Pools it may be a desired choice to reboot PFSense. On reboot you may want to test your Load Balance and Fail Over configurations. The fail over option can be simulated by either unplugging the Ethernet patch lead or turning off the power from each ADSL Router independently one at a time and testing Internet access. To test Load Balance you can use a website that replies to your IP Addresses. http://dynamic.zoneedit.com/checkip.html if you refresh the page it will give you your alternate IP Address. Another way to test the Load Balance is to have two or more users on the LAN and search for a Web Page at the same time. They should take alternate paths.

Remote Console AS much of PFSense is able to be configured by Web Browser, some other options may be to use a Remote Console Utility called "Putty and WinSCP3". These utilities are free downloads and are able to access PFSense remotely. Putty is a remote console, while WinSCP3 is an Explorer styled remote access tool. To access PFSense remotely using either of these tools, on the System Menu is the Advanced Option. Select it and on the Page is Option to enable SSH (Secure Shell). To use them use the admin name and the password that you saved.





System: Advanced functions

Note: the options on this page are intended for use by advanced users only.

Enable Serial Console

☐ This will enable the first serial port with 9600/8/N/1
Note: This will disable the internal video card/keyboard

Save

Secure Shell

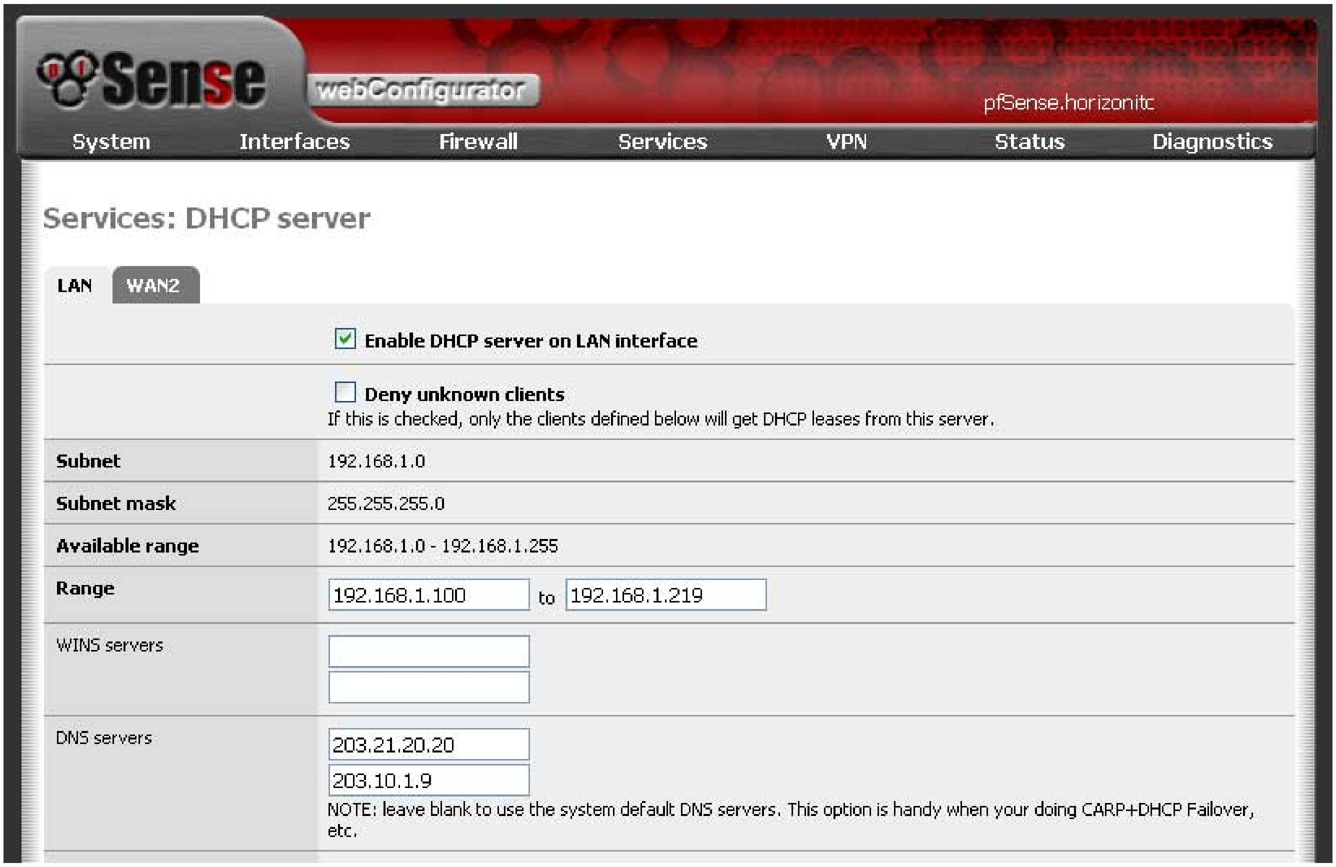
☑ Enable Secure Shell

SSH port
Note: Leave this blank for the default of 22

Save

DHCP Server It is advisable in your DHCP server to enable it and to set the DNS that you want your LAN Clients to use. The DHCP will also issue the default of DNS Address of 192.168.1.1 if no other DNS Addresses are specified. It is advisable to use the DNS Addresses that your ISP has issued your accounts.

Another option might be if you have a particular user or devices that need a set IP Address that does not change may be to dedicate an IP by Mac Address association and NetBIOS name. PFSense DHCP will never give out that IP Address to any other machine except to the one with that MAC Address. The MAC Address or each is unique, unless it is being replicated by using spoofing tools. The easies way to find the MAC Address of device is by using the ARP command found in the Diagnostic Menu or in the command console enter the command arp –a. Allocate these MAC Addresses an IP Address outside of the DHCP IP Address List and each time that device logs onto the LAN, it will be issued the IP Address allocated by MAC Address.



Services: DHCP server

☑ Enable DHCP server on LAN interface

□ Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.0 - 192.168.1.255
Range	192.168.1.100 to 192.168.1.219
WINS servers	
DNS servers	203.21.20.20 203.10.1.9 NOTE: leave blank to use the system default DNS servers. This option is handy when your doing CARP+DHCP Failover, etc.

Troubleshooting Using the command console is a good option for troubleshooting Network and Internet faults. Use the "ping and tracert" commands will assist you in diagnosing your problems. In the Diagnostic menu the ping function is available to ping through each Interface, LAN, WAN and OPT Interfaces. First try pinging your WAN gateway and then your Monitor IP through your WAN. If no problem exists there, then ping through your OPT Interface the OPT gateway and monitor IP. These are just a couple of simple troubleshooting techniques. For PFSense assistance please refer to the PFSense Forum, Support List and Archives.
If loss of Internet still persists, connect your ADSL Routers directly to a client and test for Internet browsing ability. Your fault may lie with your Router Setup or incorrect WAN, OPT patching to WAN and OPT interfaces.