

# Multiple Subnets on One Interface in pfSense

This document describes how to configure multiple IP subnets on a single interface in pfSense.

First, make sure the single subnet configuration is fully functioning as you desire. Then proceed with the following to add the second subnet. This document assumes you are using the LAN interface to add an additional IP, but this will work for OPT interfaces as well.

## Adding the Additional IP to the Interface

This will be possible entirely in the GUI in 1.3, but for now it requires a little manual hacking.

Log into the webGUI, and click Diagnostics -> Backup/Restore. Click the "Download configuration" button. Open the xml file downloaded in a text editor, like Notepad. Above the </system> line, insert the following:

```
<shellcmd>ifconfig fxp0 inet 192.168.2.1 netmask 255.255.255.0 alias</shellcmd>
```

Replacing fxp0 with the name of the interface you're using, and the IP and subnet mask as appropriate. You can find the name of the desired interface in the config file. For example, for LAN, see this portion of the config.

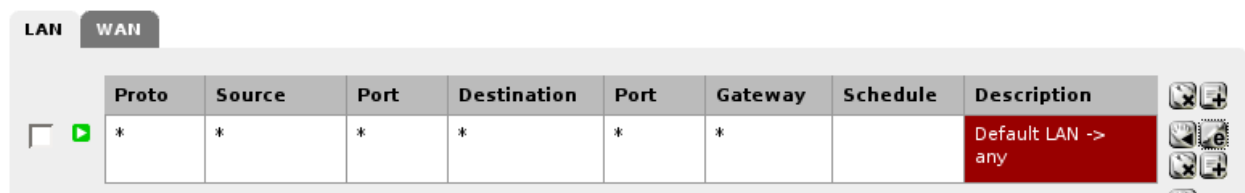
```
<interfaces>
  <lan>
    <if>fxp1</if>
```

This is showing the LAN interface as fxp1.

Save the configuration change, go back into your pfSense webGUI backup/restore screen, and restore the changed configuration. The firewall will reboot.

## Modifying the Default Firewall Rules

The default LAN rule only allows traffic sourced from the LAN subnet. You either have to edit the default rule and change the source to any, or add a second rule on the LAN permitting traffic sourced from the second subnet. Both examples shown below.



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

LAN WAN

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
<input type="checkbox"/>	*	LAN net	*	*	*	*		Default LAN -> any
<input type="checkbox"/>	*	192.168.2.0/24	*	*	*	*		Second LAN subnet -> any

### Modifying the Default NAT Behavior

pfSense automatically generates your NAT rules behind the scenes. That won't work in this scenario. Click Firewall -> NAT, Outbound tab.

Select "Manual Outbound NAT rule generation" and click Save. A NAT rule for your primary LAN subnet will automatically be added. Click the + to the right of "Auto created rule for LAN" to add another NAT rule based on that rule. Change the source network to your second subnet, and click Save. Then click Apply Changes.

Port Forward 1:1 Outbound

Automatic outbound NAT rule generation (IPSEC passthrough)

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

**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
<input type="checkbox"/>	WAN	192.168.1.0/24	*	*	*	*	*	NO	Auto created rule for LAN
<input type="checkbox"/>	WAN	192.168.2.0/24	*	*	*	*	*	NO	LAN 2

You should now have two working subnets on a single interface.