Setting up pfSense as a Stateful Bridging Firewall.

Contents

Contents

What king of system these directions will try and help you create.

- The goal of this page is help you setup a pfSense firewall, with the following features:
  - Bridging firewall, not a NAT firewall
  - QoS/Packet shapping to avoid saturation of your Frodo link with low priority traffic
  - Intrusion prevention using SNORT (optional, see further documentation)
  - Firewall rules to block undesirable traffic.
  - Integration with Oxford services, such as NTP and DNS (hum drum stuff)

This documentation still isn't complete yet!

Selecting your server.

You have two rough options with servers:

Option 1 – Basic stateful firewall.

> You won't need a very high spec system for this (unless you are expecting it to pass a lot of traffic, say over 1Gb/s). We had a PIII based server doing the job on our 100Mb/s connection without any load problems.

You'll need 3 NICs, Some sort or processor (ideally 64bit). 512Mb or more of RAM and a few Gb of disk space.

Option 2 – Intrusion prevention firewall.

For this setup, you'll need a bit more processing power, as the intrusion prevention/detection program (SNORT) uses a fair amount of power.

I'd recommend a Quad core processor, such as a Xeon with 1Gb or more of RAM.

Again you'll want 3 NICs. You'll also want a few Gb of disk space.

Installing pfSense

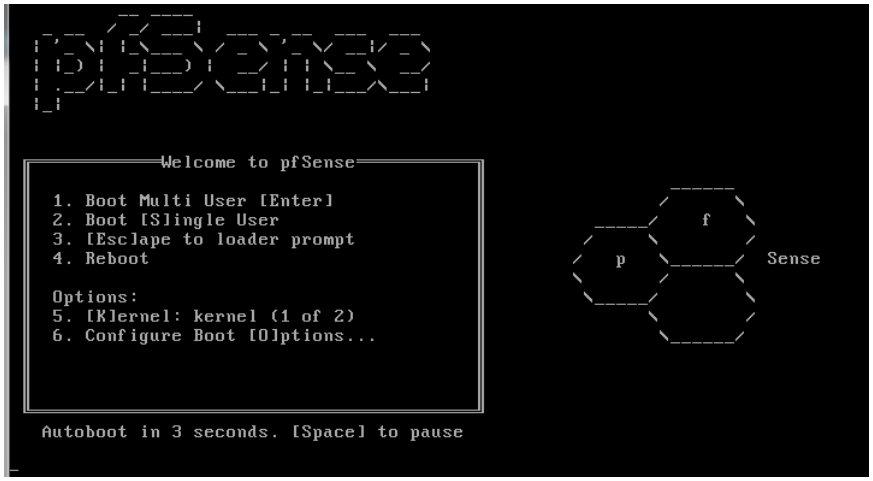
Download a copy of the pfsense ISO from
https://www.pfsense.org/download/mirror.php?section=downloads

You'll almost certainly want to use the 'Live CD with Installer' platform, unless you plan to create your own pfSense applicance (out of the scope of this guide).

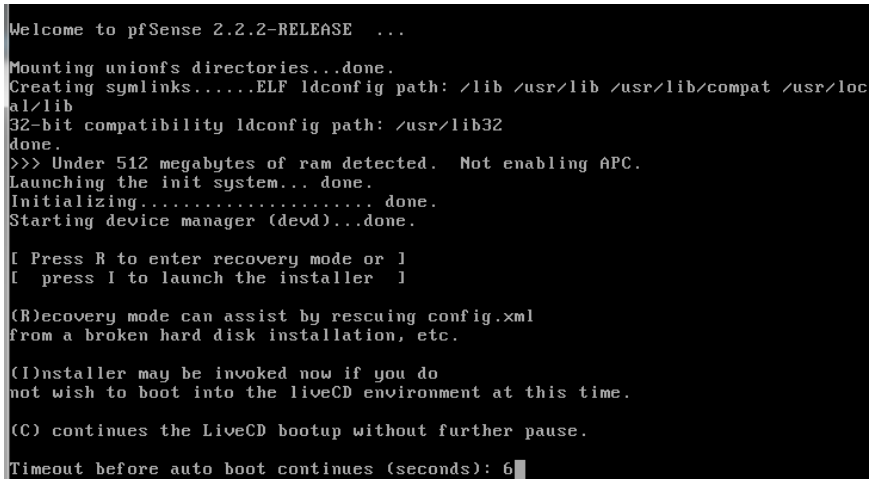
Select the correct 32/64bit version of pfSense to match your server.

NB. You may find that pfSense can cause problems with existing firewalls (such as Watchguard), when used in bridge mode.

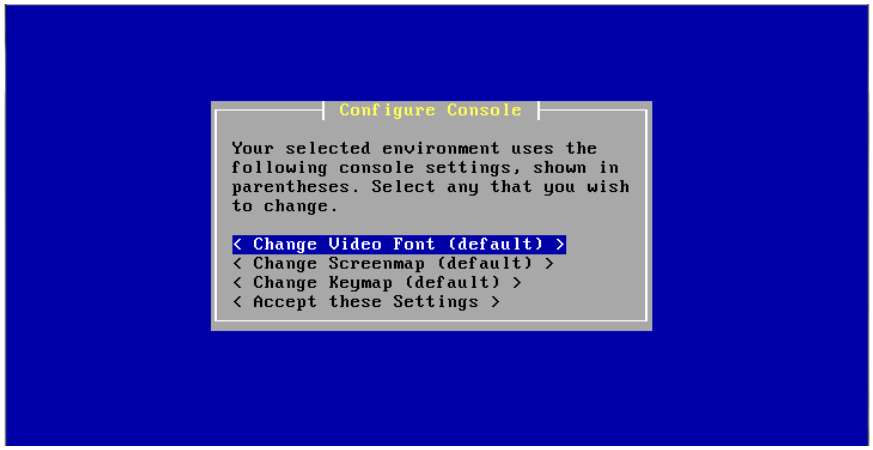
Once you've downloaded the ISO and burnt it to CD, boot your server and you should see:



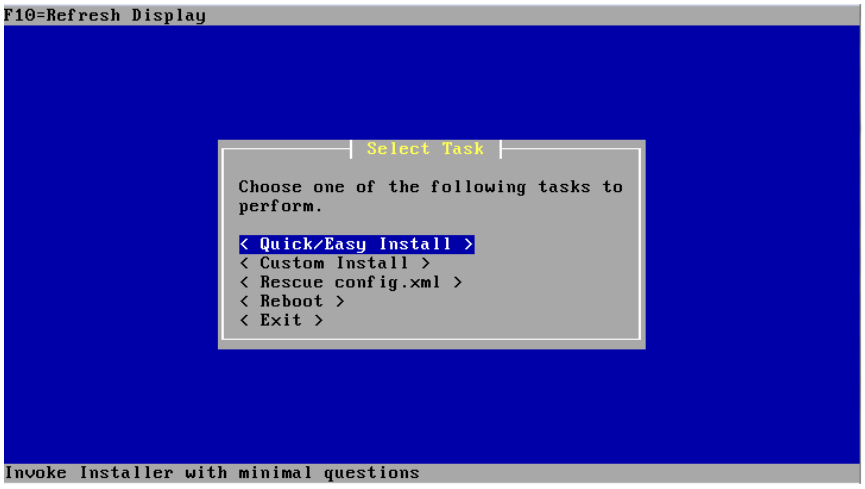
Then you'll get to an options screen which will give you the option to install if you press 'i':



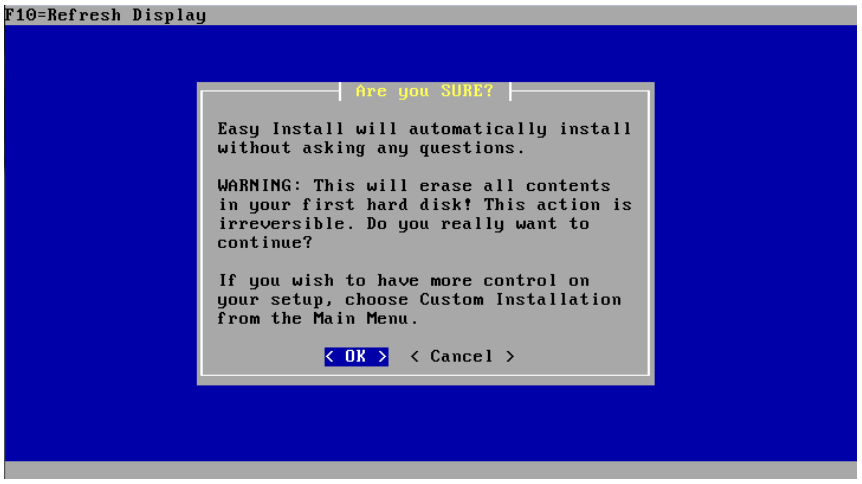
Pressing ‘i’ gets you to a configure, select ‘accept thease settings’:



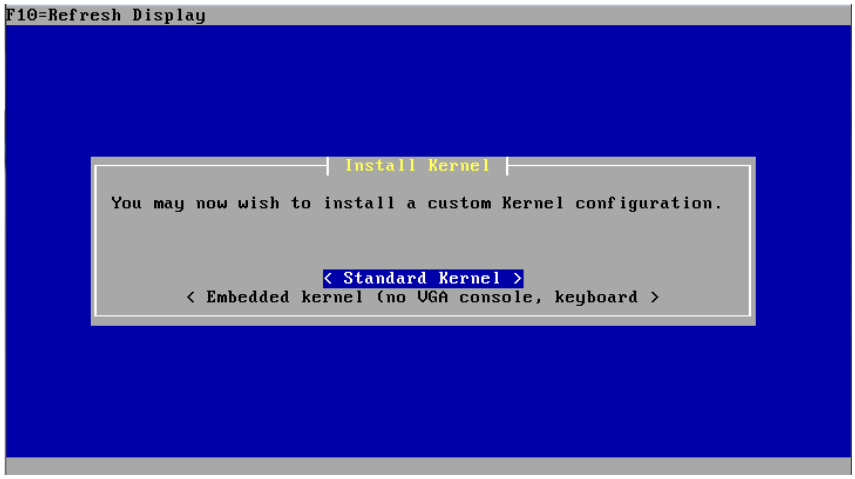
Then select ‘Quick/Easy Install’:



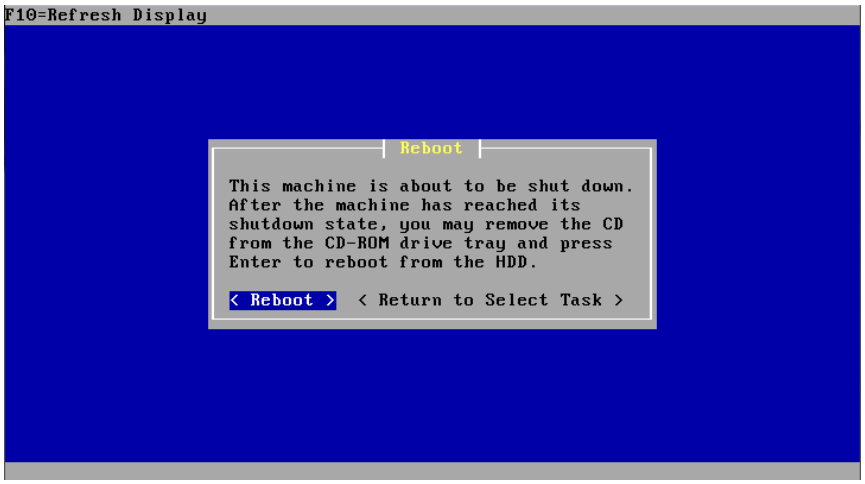
Accept the fact you server’s disks will be formatted and the data (if any) will be lost:



Wait a brief moment as the partitioning occurs, then select ‘Standard Kernel’:



That's the installation done:



Don't panic when booting, the boot loader screen is quite minimal and will continue booting after a few seconds:

Once pfSense has loaded you should end up with a console menu like this:

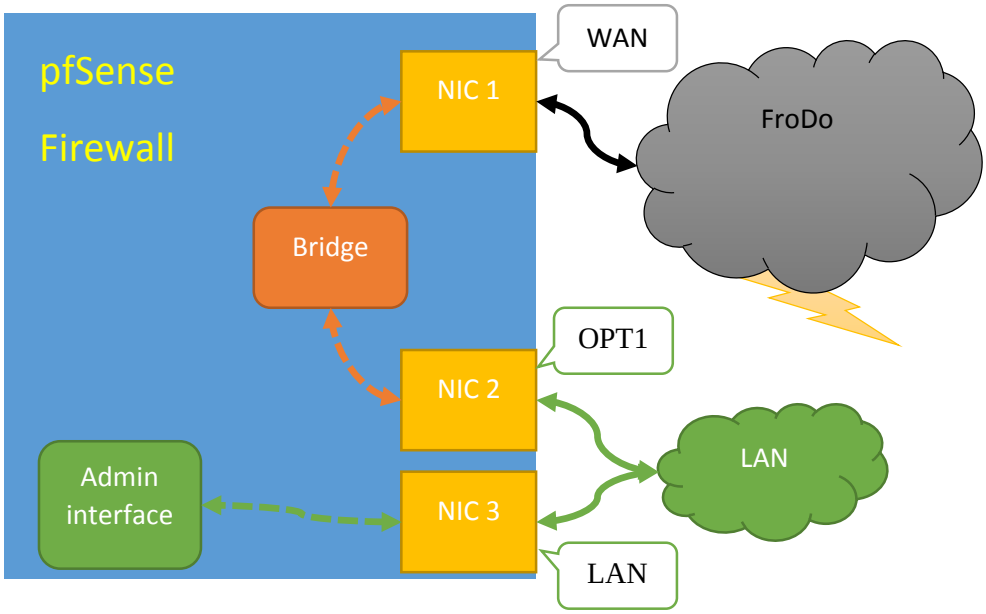
```
Configuring firewall......done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.2.2-RELEASE amd64 Mon Apr 13 20:10:22 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        ->
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Setting up the basics (IP assignment, etc)

The first task is interface assignment.

Your newly installed pfSense firewall comes with the notion of a LAN and WAN interfaces.

You'll also want to add a management interface and turn on bridging (a bit later), so that you end up with something like this:



From the previous diagram, we have the WAN interface connected to NIC number 1, which we'll connect to the FroDo/outside world.

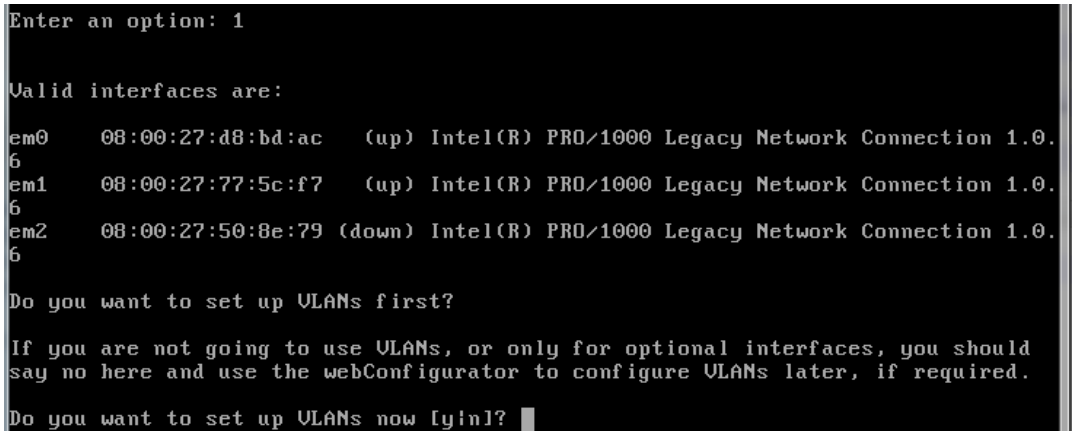
Then we have the 'OPT1' interface connected to NIC number 2, which we'll connect to our LAN switches.

Finally we have the 'LAN' interface, which we'll use purely for administration, which we can also connect to the LAN switches. Using a separate interface for managing the firewall helps avoid accidently being locked out of the firewall due to misconfigured firewall rules and problems with IP assignment of interfaces on the bridging interfaces (more on that later).

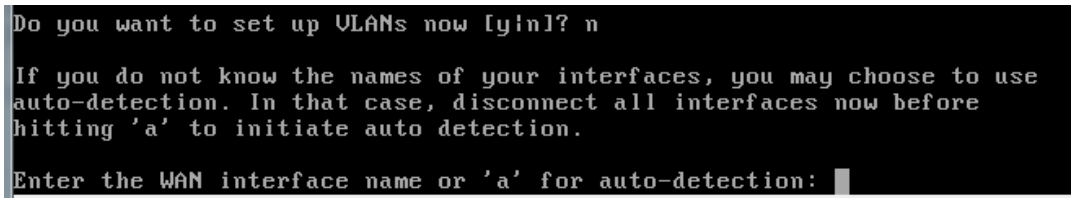
You'll need to work out which interface pfSense thinks is which (which may not be in the order you might expect).

Fortunately pfSense allows you to 'detect' which interface is which.

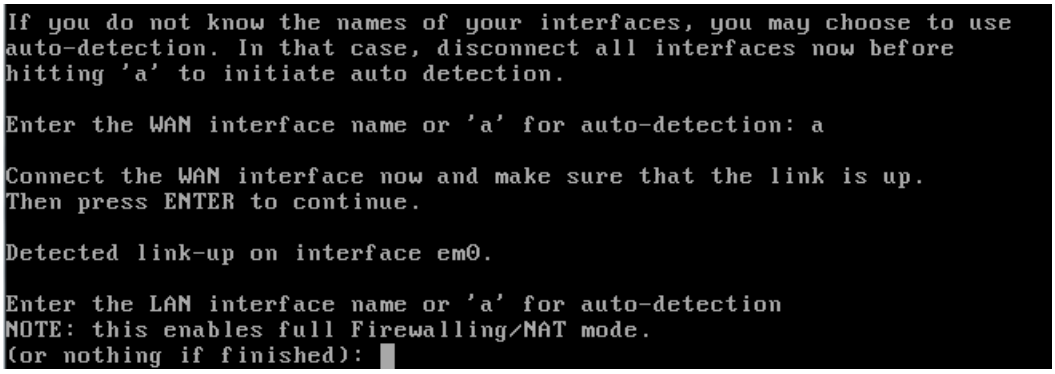
Select option '1' – assign interfaces:



Select 'n' for no VLANS and then select 'a' to autodetect the NIC to be assigned as the 'WAN' interface:

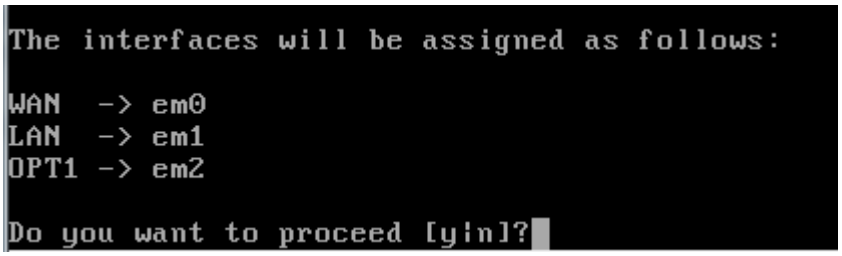


Plug a cable into the NIC on the server you wish to use for the 'WAN' and pfSense will detect the port change and assign that NIC as the WAN (you may want to label the port).



Once you've assigned the WAN interface to a NIC, you can continue in the same way with the LAN and OPT1 assignments.

Once the interfaces are assigned you should have a summary of the assigments for you to confirm:



NB. If the auto detection doesn't work for you, then you can always fill in the values of the detected NICs and work out which is which later.

pfSense labels Intel NICs as "em#", "igb#" or "ix#" where the '#' is the number of the NIC, starting at 0.

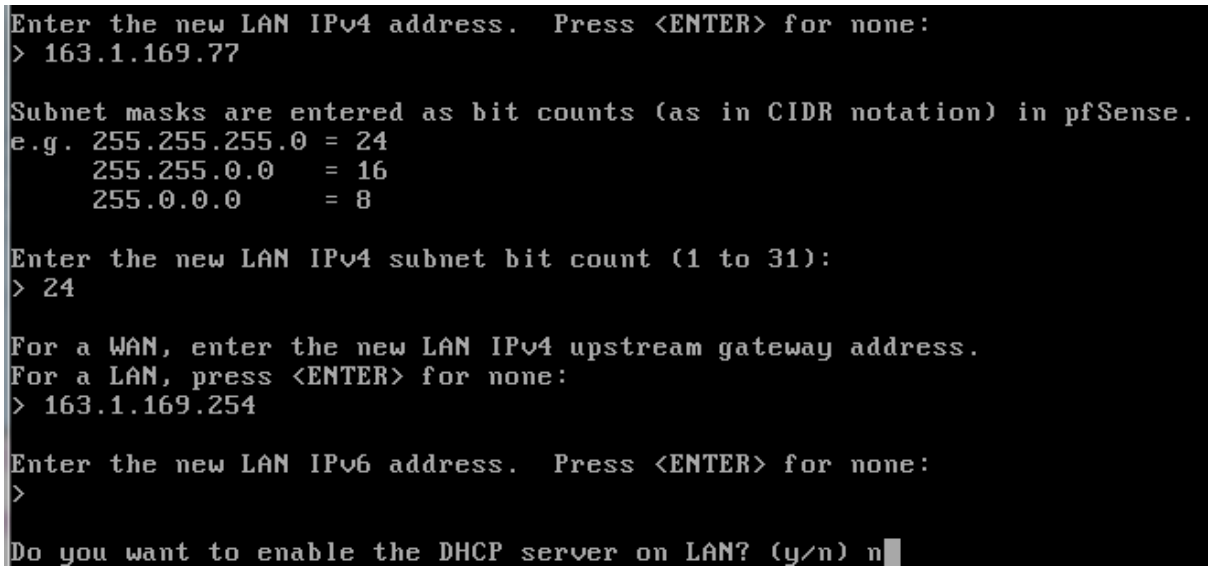
It also labels Broadcom NICs as "bge#" or "bce#", again where the '#' is the number of the NIC, starting at 0.

Assigning an IP for web management.

The console menu is quite limited and only a first step to setting up the firewall, now we need some admin connection to allow us to manage the firewall via a browser.

Select option '2' – Set interface(s) IP address.

You'll get asked which interface you want to change it's IP assignment for – go for LAN, as this is going to be our management interface.



Enter an IP address, subnet mask and gateway/router IP.

Then press enter for no IPv6 address.

Make sure you *disable* DHCP when asked.

When asked if you wish to revert to HTTP you should say 'n'.

Then press enter to continue after you've made a note of the URL.

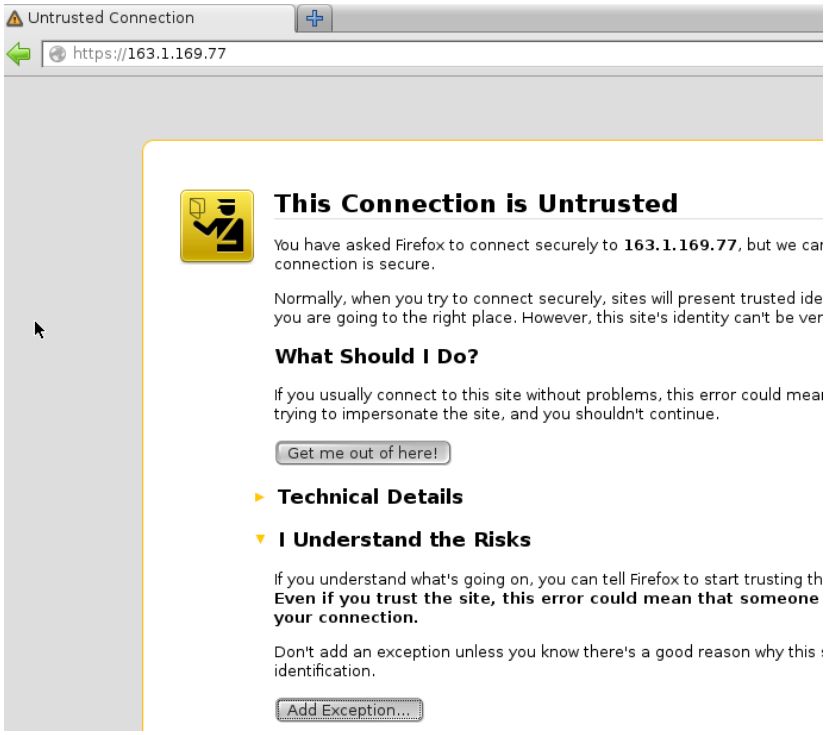
More configuration with a browser.

Now we should have access to the firewall with a web browser.

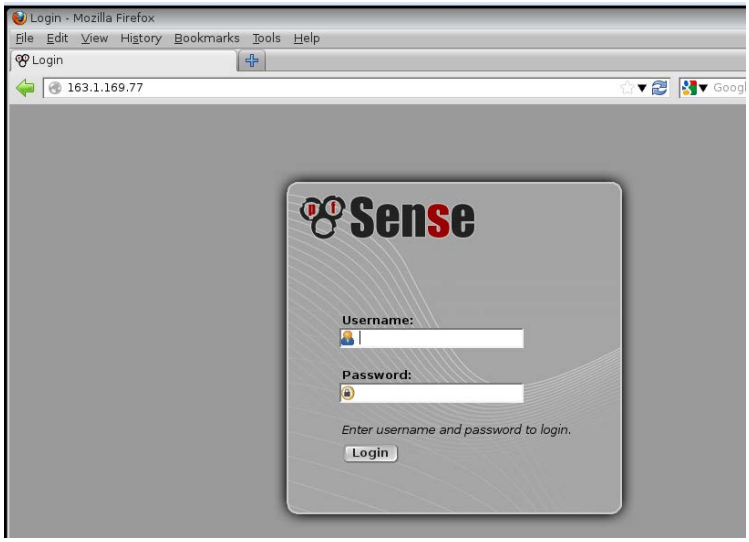
Our first task is to logon and change the admin password.

You should be able to open session to the firewall, using the IP of the firewalls LAN interface (so long as the machine is connect directly or by a switch to the NIC assigned to ‘LAN’).

You’ll be presented with a warning (depending on your browser):



As the ssl certificate will be a self-signed one – you’ll need to obtain a signed certificate from IT Services to avoid this. Bypass this for now.



Logon with the default password and username:

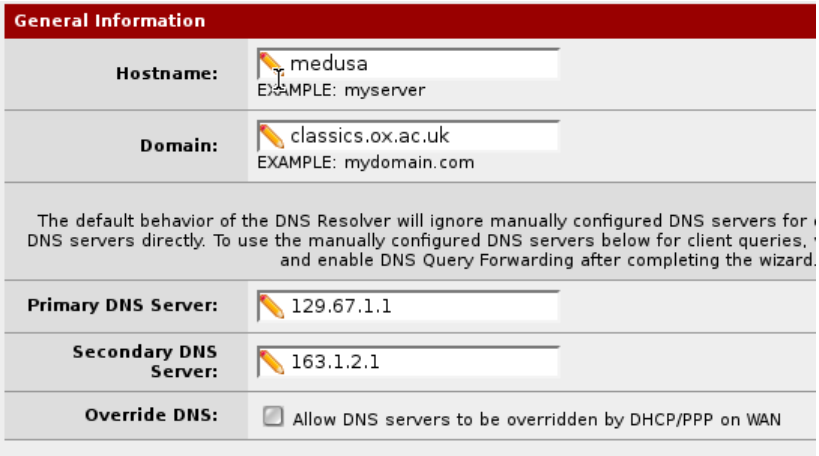
Default username: admin

Default password: pfsense

You'll then get a wizard to guide you through more of the initial configuration of pfSense.

Click next and next again past the subscription advert.

Now you can set the host name, domain and DNS servers:

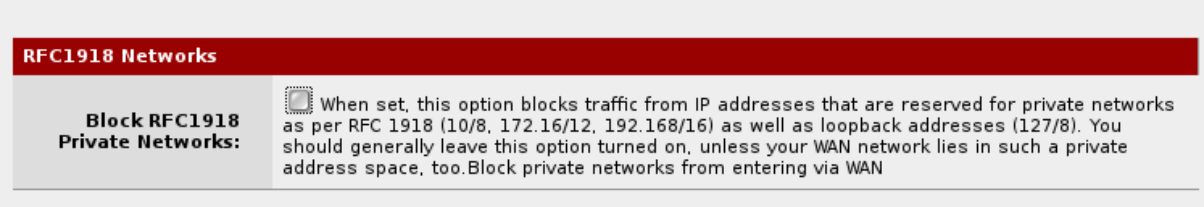


NB. Uncheck the 'Overide DNS' box at the bottom.

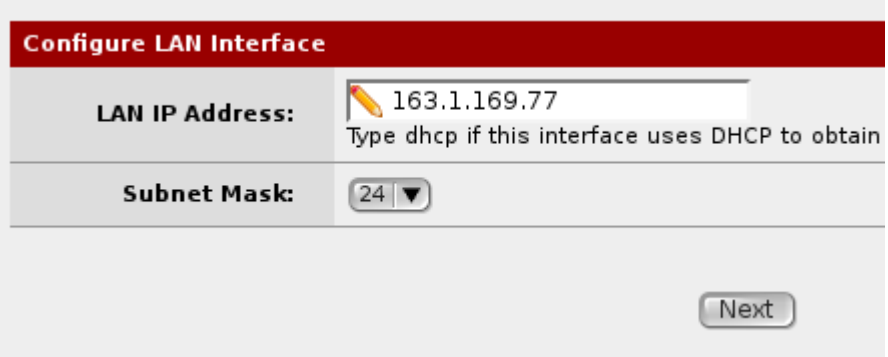
The next screen allows us to setup the timezone and an NTP server:

The Wide Area Network (WAN) should be configured to have *no* IP assignment, but we'll leave this set to DHCP for now.

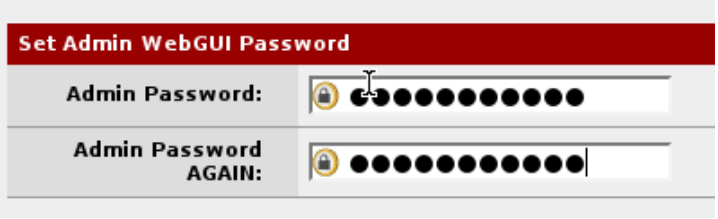
You may want to uncheck 'block RFC1918 Networks' at the bottom though:



The next screen is to configure the LAN interface, just click next for now:

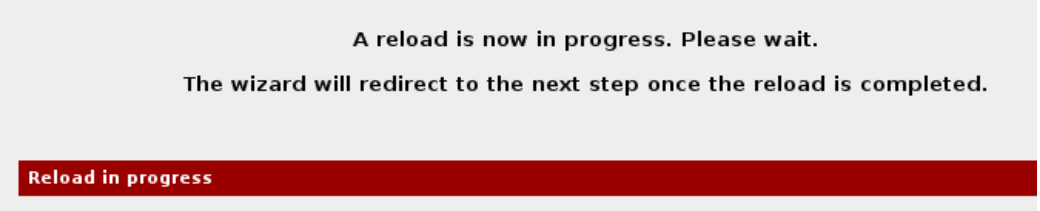


Finally you can set a password for the firewall:

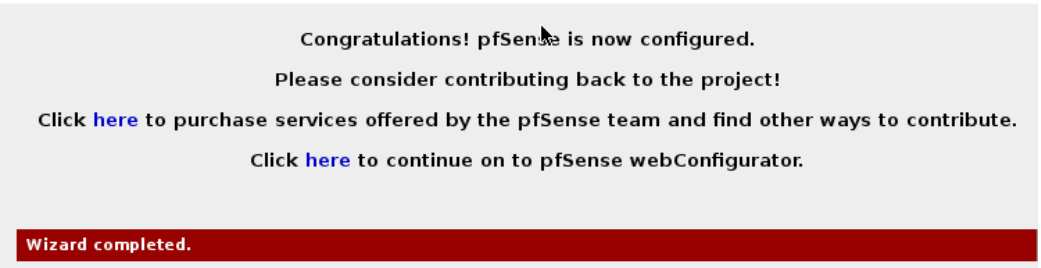


NB. This password is for the admin user, not just the web admin console.

Then you'll be prompted to reload the firewall with the new settings:

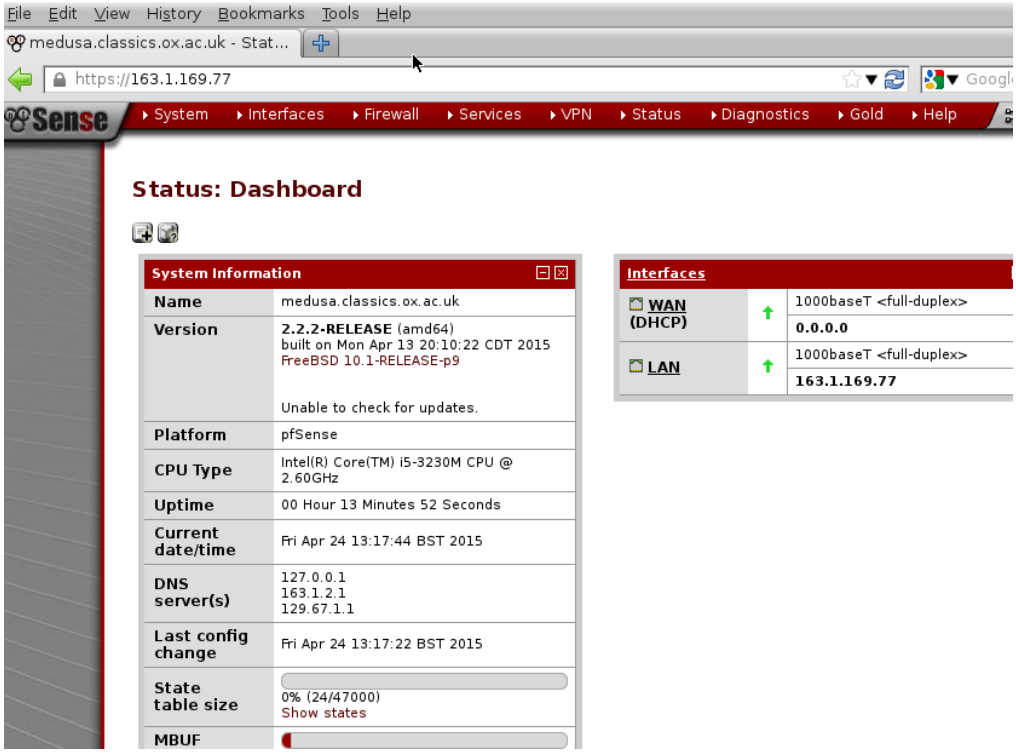


…



Done.

You should be taken to the ‘dashboard’ for the firewall when you click the ‘click here’ to continue link (shown above):



How to setup bridging mode

By default the firewall works in NAT mode. (NB. If you wish to keep pfsense as a NAT firewall you may want to check it will log enough information to make OxCERT happy and ensure you are within the university rules - see http://help.it.ox.ac.uk/sites/ithelp/files/resources/network_security_nattalk.pdf as well as http://help.it.ox.ac.uk/network/security/logging).

To change to bridge mode you need to:

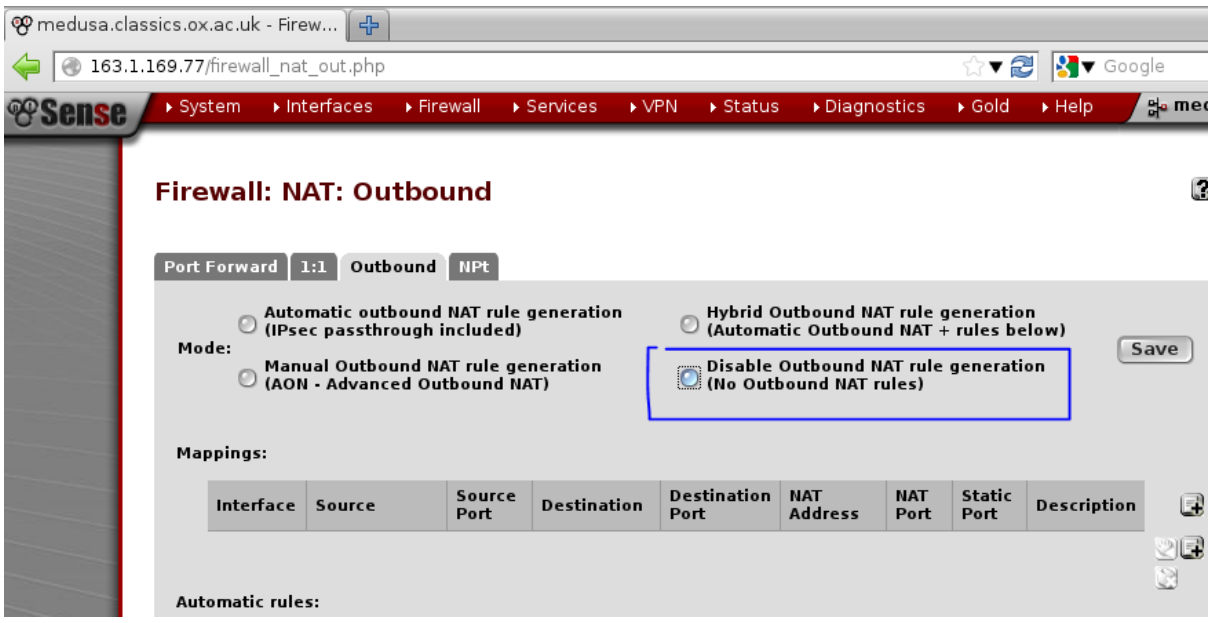
- Disable the auto-creation of NAT rules
- Change the WAN and OPT1 interface configuration
- Create a bridge between two interfaces
- Check your filtering options

Disable the auto-creation of NAT rules

Goto the menu bar, click on the firewall drop-down menu and select 'NAT'.

Then select the 'NPt' tab:

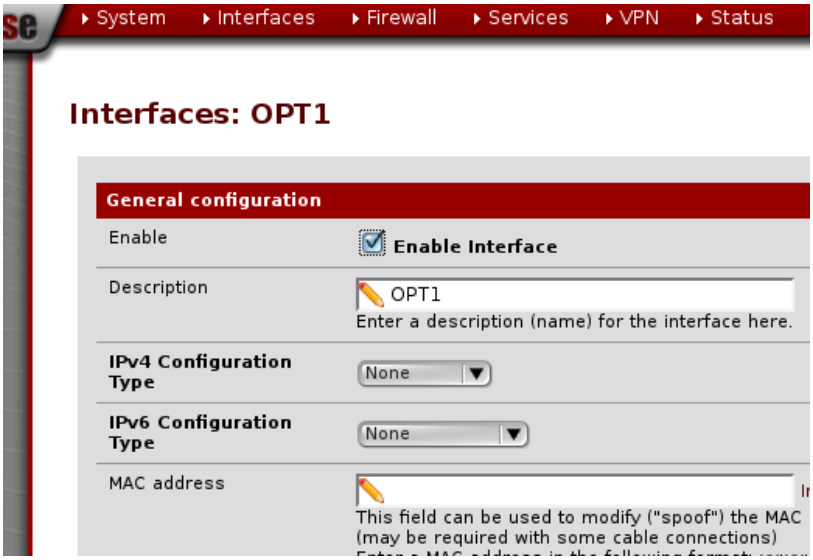
Disable the automatic creation of NAT rules and click the save button.

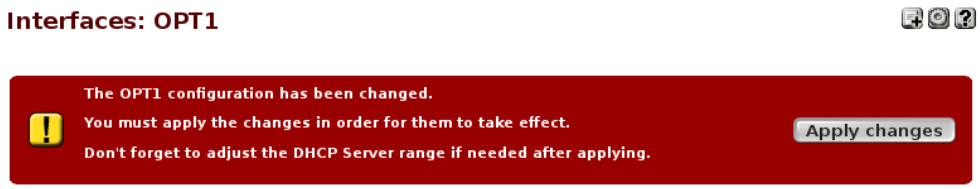


Change the WAN and OPT1 interface configuration

Now select the drop down menu ‘interfaces’ and select ‘OPT1’:

Check ‘enable interface’ and then save:

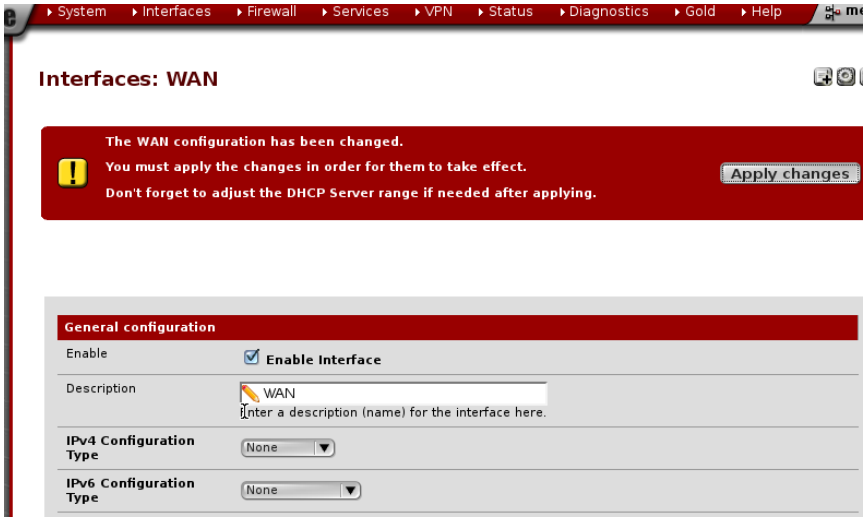




You’ll also need to ‘apply changes’ made.

Goto the interfaces drop down menu and select WAN.

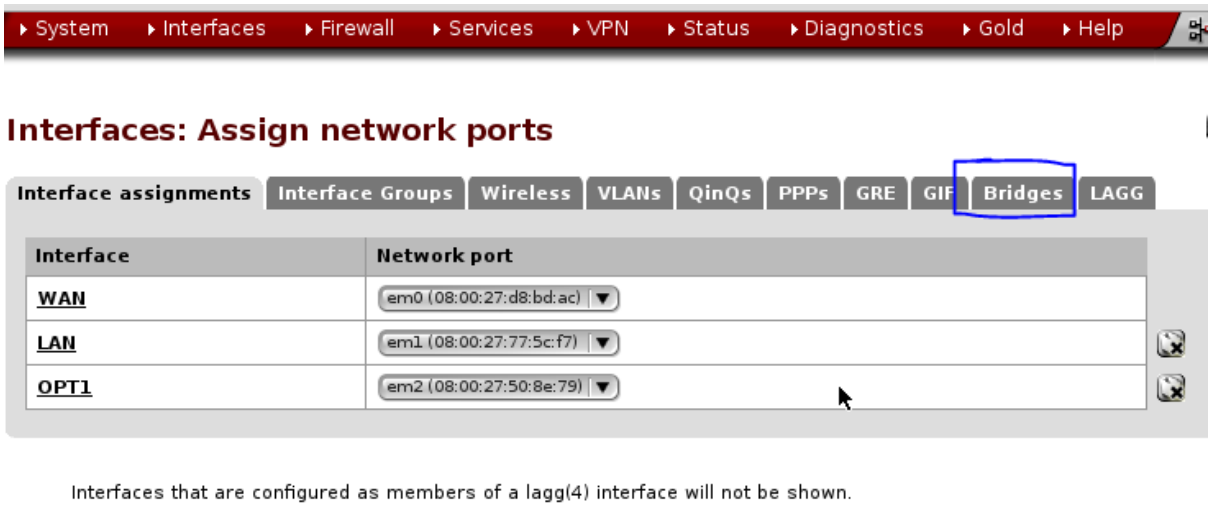
Change the IPv4 and IPv6 configuration types to ‘none’



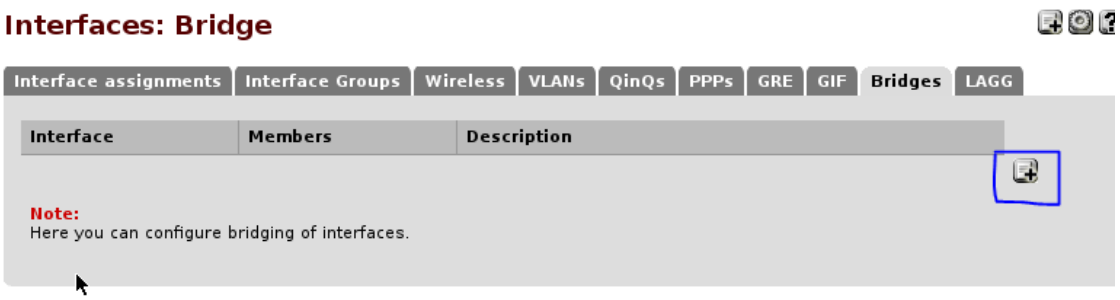
Click save and apply the changes.

Creating the bridge interface

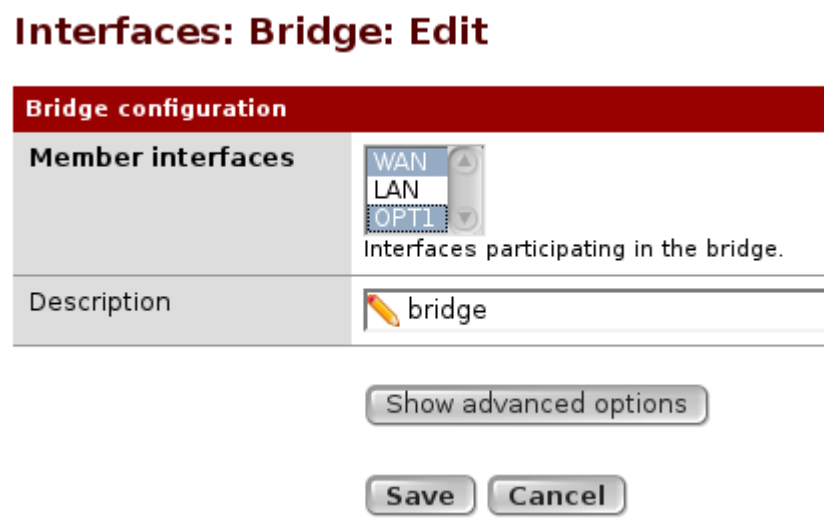
Go to the 'interfaces' drop down menu again and select 'assign', then select the 'bridges' tab:



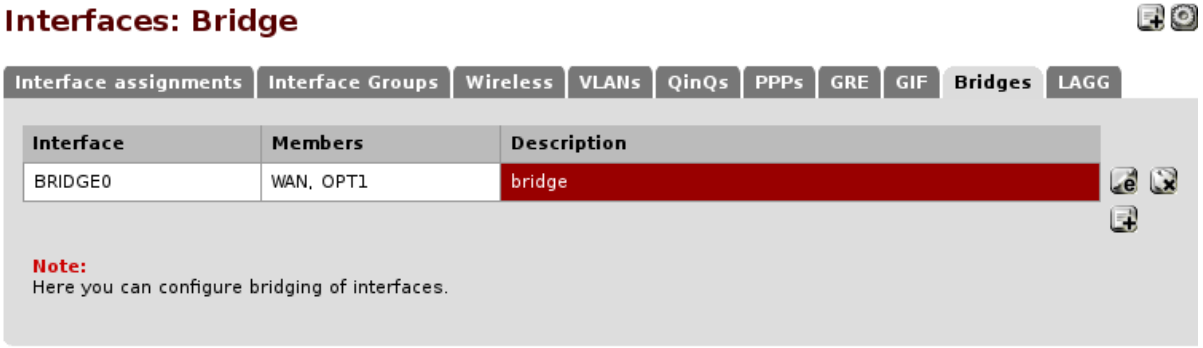
Click on the small '+' icon to add a new bridge:



Select the interfaces to be in the bridge (OPT1 and WAN) and give the bridge a simple name:



Click save and you should have a bridging firewall!:



Checking the filter options

By default the filtering of traffic should be set on OPT1 and WAN, not the bridge as well.

To check this is the case, goto the ‘system’ drop down menu and select advanced, then the ‘system tuneables’ tab.

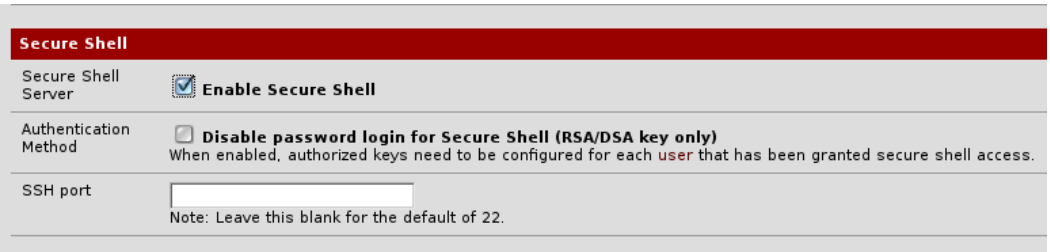
Ensure the following options are set:

net.link.bridge.pfil_onlyip	Only pass IP packets when pfil is enabled	0
net.link.bridge.pfil_member	Packet filter on the member interface	1
net.link.bridge.pfil_bridge	Packet filter on the bridge interface	0

Packet filtering on member interfaces and the bridge interface can lead to strange and hard to diagnose behaviour from the PF firewall.

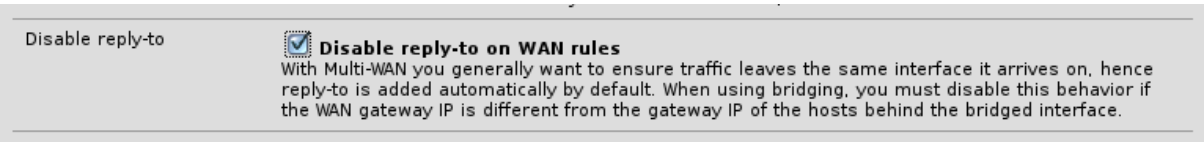
Yet more configuration

Enable SSH (for system tuning later) with ‘System’ -> advanced -> Admin access:

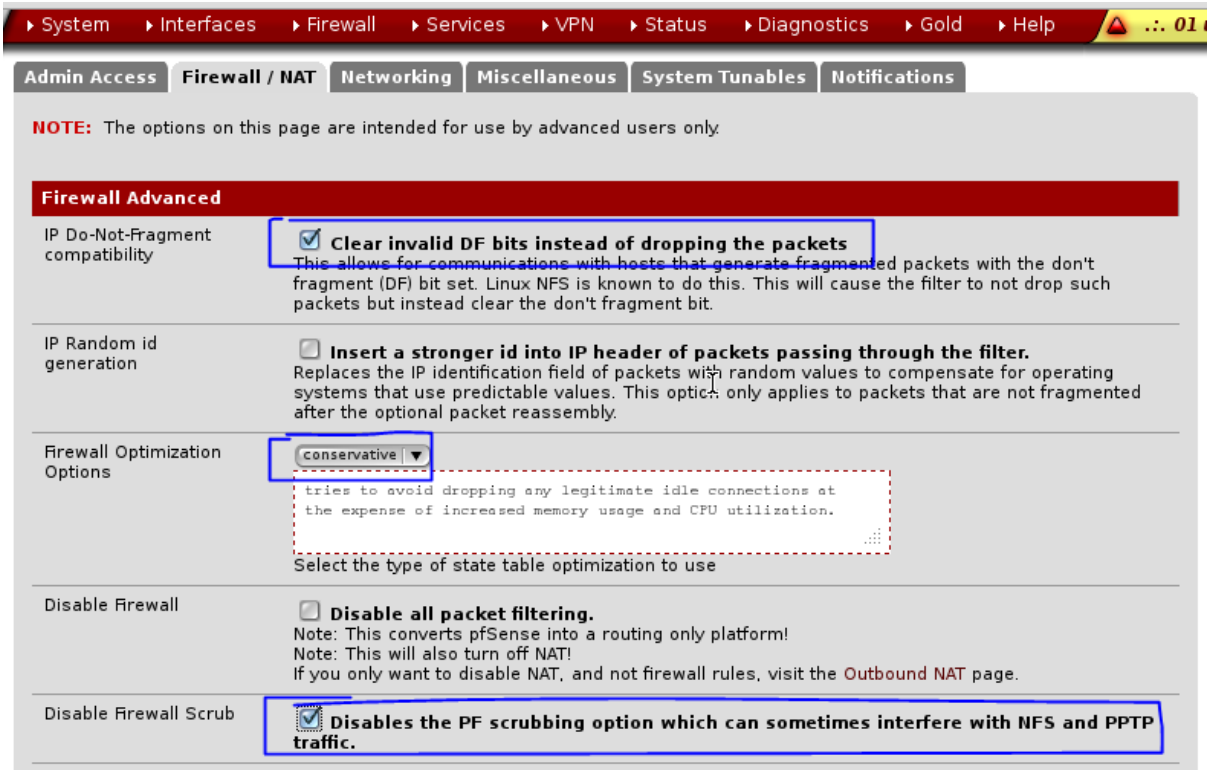


Save those changes.

Turn off ‘reply to’ for NAT as we’re using a bridge instead with System -> Advanced -> Firewall/NAT:

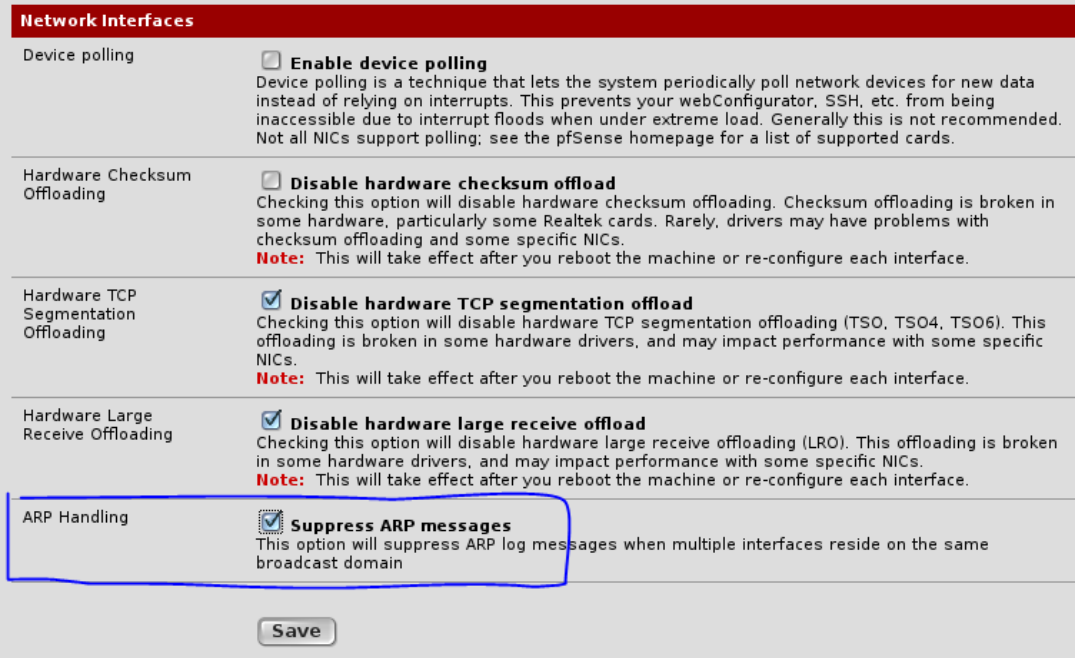


On the same page we have the following options set to avoid problems with fragmented packets:



Click save.

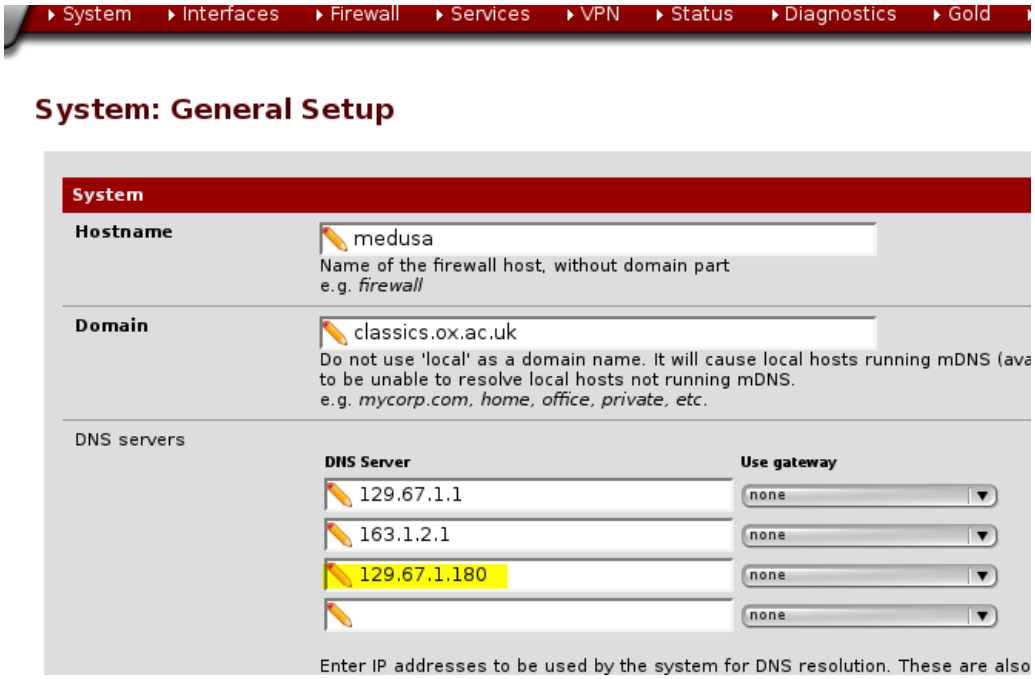
Then click on the ‘networking tab’ to set ‘ARP Handling’ (at the bottom of the page):



Make sure you save again…

Adding a third DNS server – System -> General setup

Enter the 3rd IT services DNS resolver:



Save your changes, as usual.

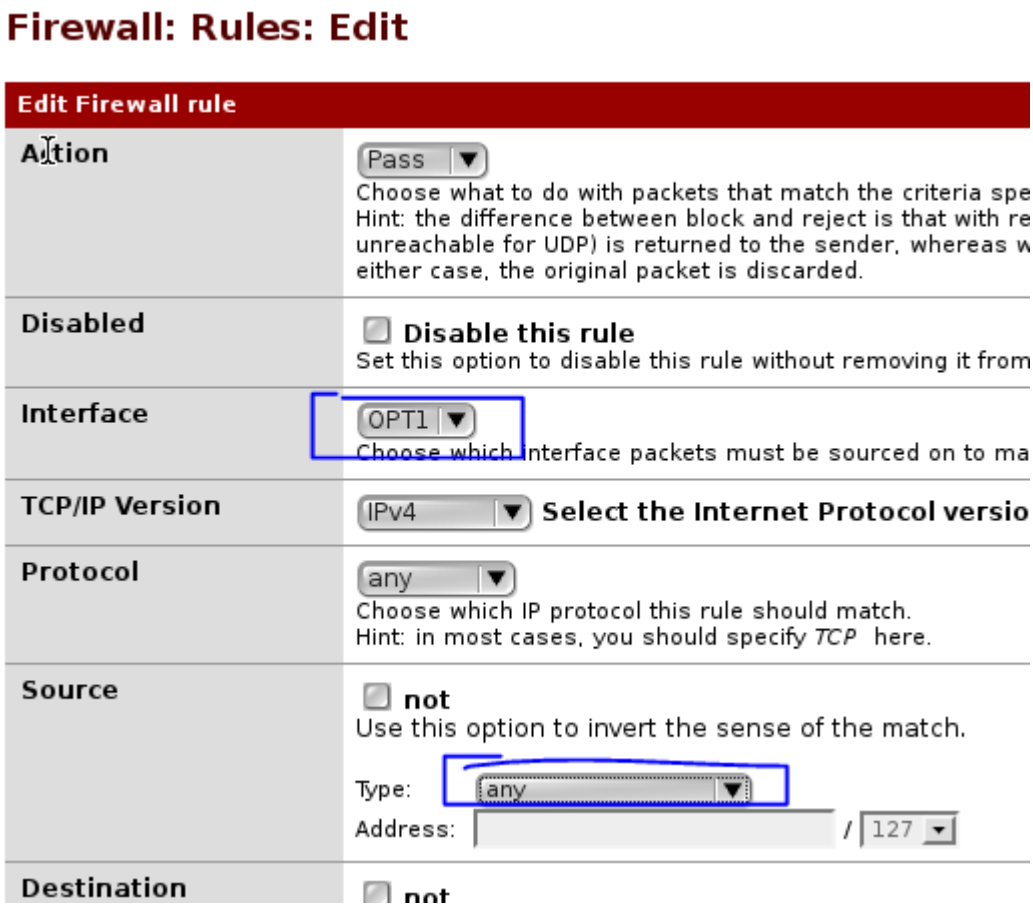
Creating firewall rules

You'll find the firewall block pretty much everything at the moment.

We need to sort out the firewall rules.

Go to: Firewall -> Rules -> LAN

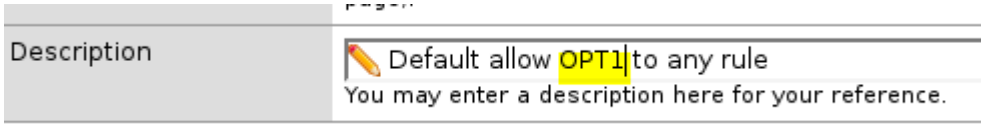
Use the '+' button on the existing IPv4 rule to create a duplicate rule:



Change the interface to 'OPT1' and the source to 'any'.

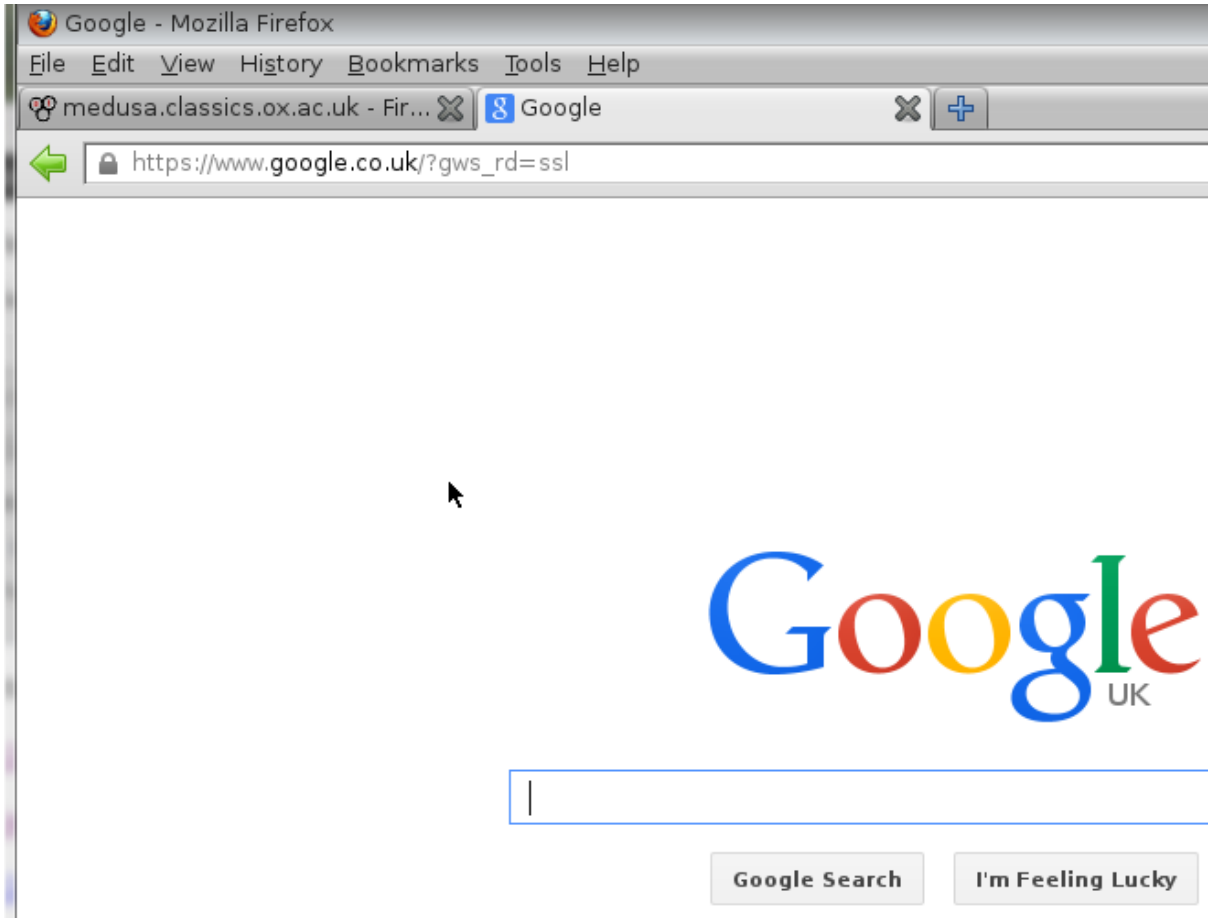
This will allow all IPv4 traffic out from our LAN via the OPT1 interface (if you want to be more restrictive, you can create individual rules for outbound traffic on the OPT1 interface.

Update the description and save:



Finally 'Apply changes'.

Now you should have a working firewall you can get at a few webpages from:



Setting up your own rules.

Aliases

Firewall rules work best when using aliases.

You can use an Aliase to refer to an individual IP/DNS address or a network range or list of IPs/Hosts.

Aliases can even refer to each other or to specific URLs (handy for virtual host filtering although processor intensive) and ports.

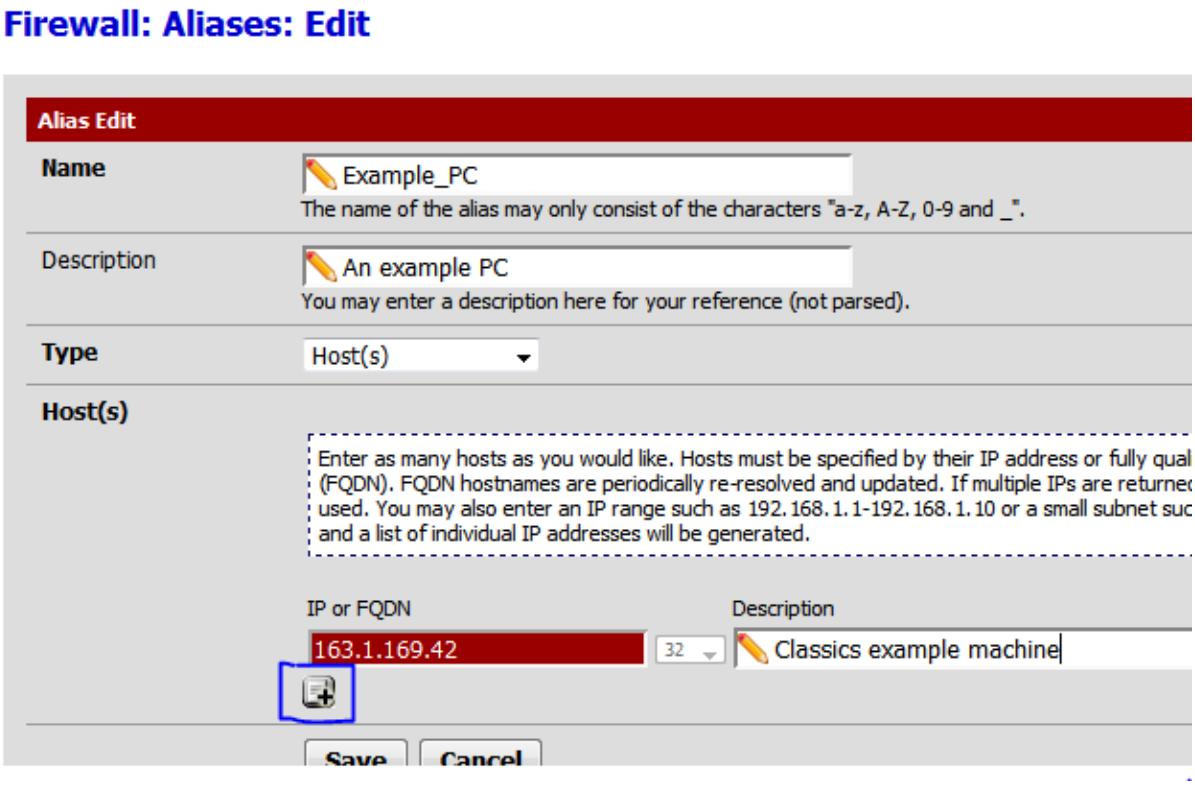
To create an alias, goto Firewall -> Aliases.

Then you'll see a list of existing Aliases (none be default):

Click on the '+' button to get to the new alias screen.

When creating an alias you're required to choose the 'type' of alias.

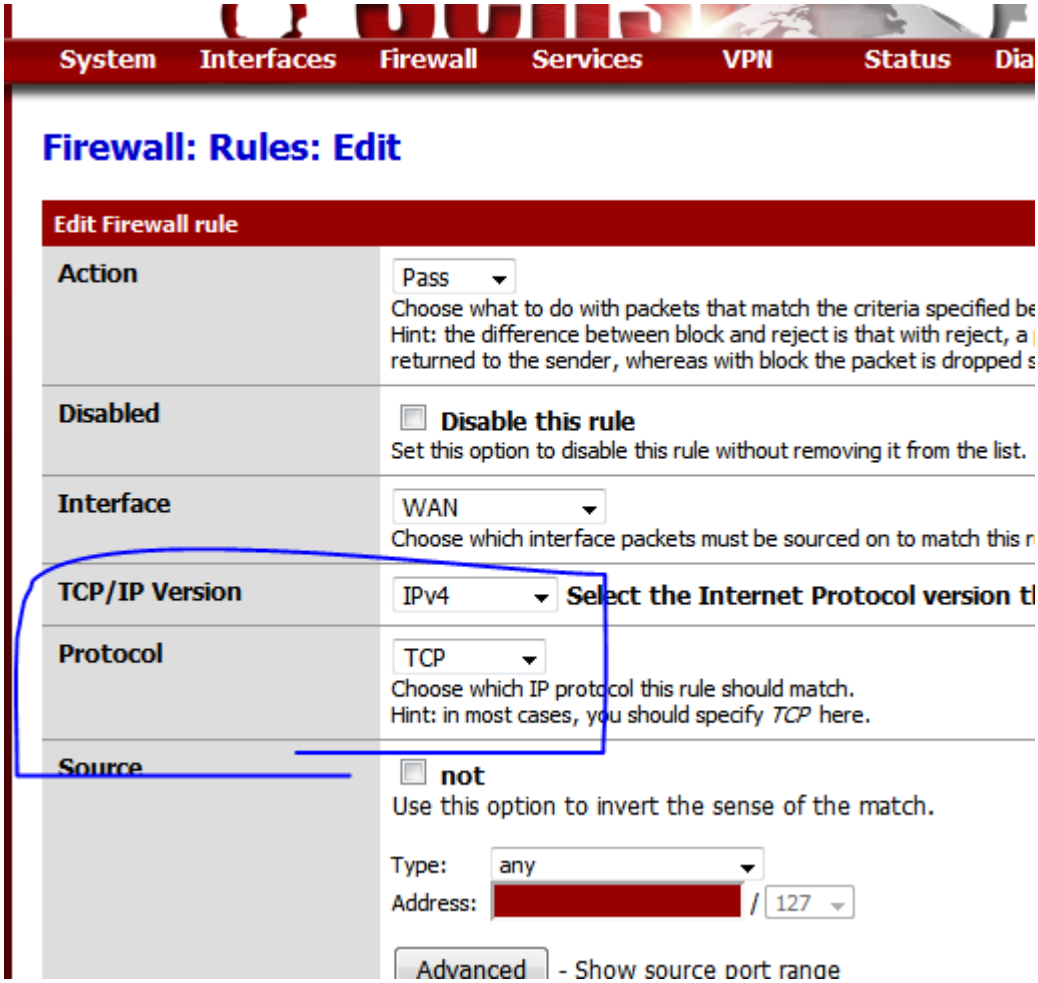
- Host(s) – IP or FQDN list of host or hosts
- Networks(s) – list of network ranges
- Ports – list of port numbers/ranges
- URL
- …



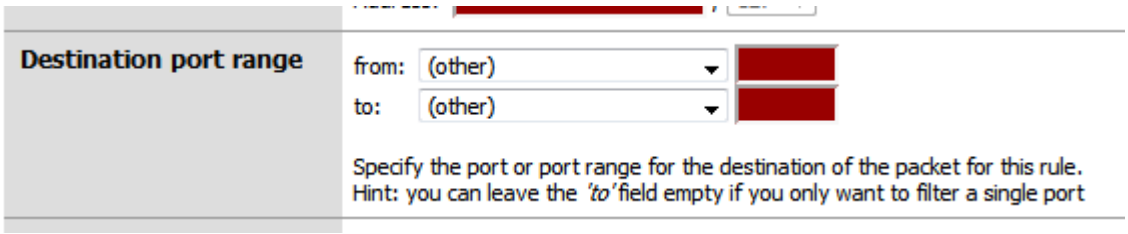
In this example a PC's IP is entered as an alias.

The '+' is clicked on to enter IPs/FDQNs and clicked on again to enter another IP/FSQN.

When creating a new rule, pay special attention to the protocol, as it's TCP only by default:

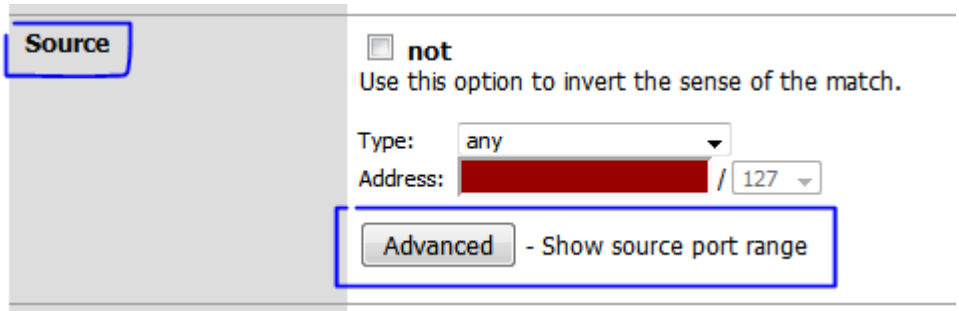


With the 'Destination port range', this can appear a little confusing:

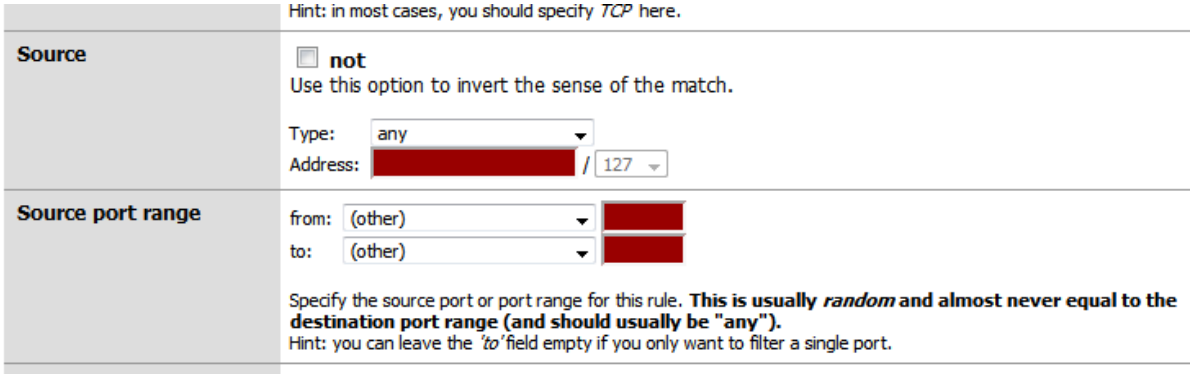


The 'from and to' refer to the port range the packets will be headed for.

To specify a rule which refers to which ports the packets have been sent from, look further up at the advanced button:



This will reveal the ***source*** port range configuration if clicked:



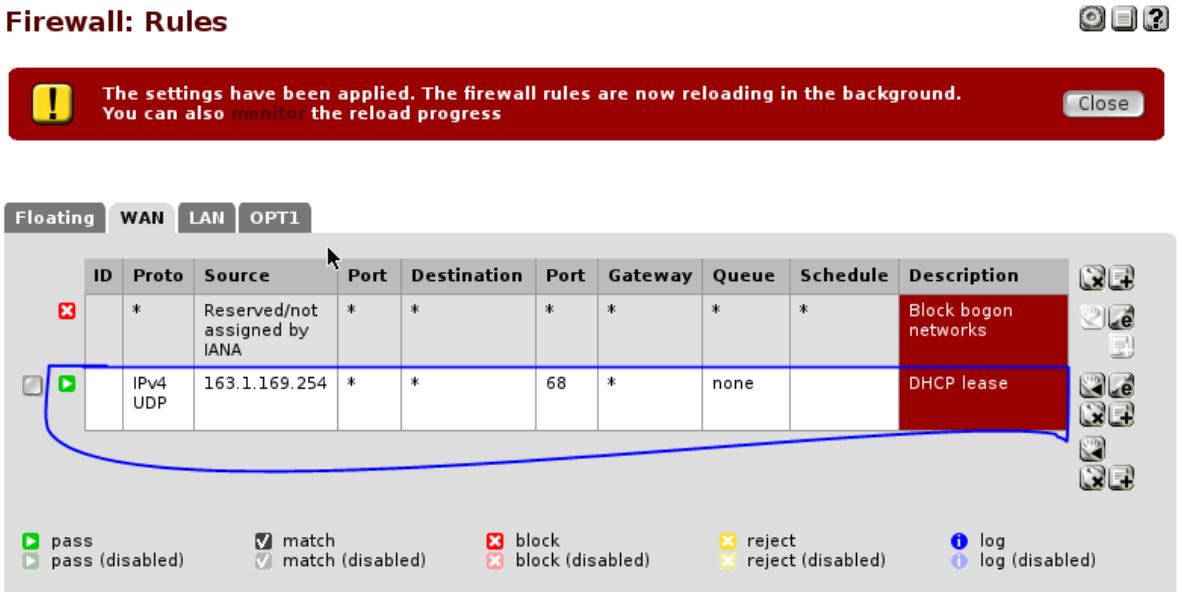
Examples - Adding other useful rules for essential IT services

DHCP (v4)

Usually DHCP requests are sent by the IP 0.0.0.0 on the LAN as a broadcast.

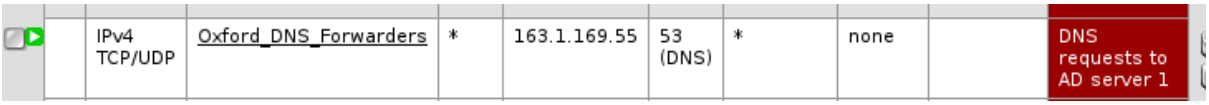
This is handled by the IPv4 pass rule on the OPT1 interface.

The return packet comes via the router:



Not the traffic type is UDP and the destination IP is not set (as the client still has the IP 0.0.0.0 at this point). The source is set as the IP of the router.

DNS resolution for Microsoft AD servers



Rule setup for Oxford forwarders to be able to query and AD server with IP 163.1.169.55

The alias ‘Oxford_DNS_Forwarders’ is the list of DNS forwarders (129.67.1.1 129.67.1.180 and 163.1.2.1)

WINS resolution

(TBC)

Monitoring your firewall

Remote syslog

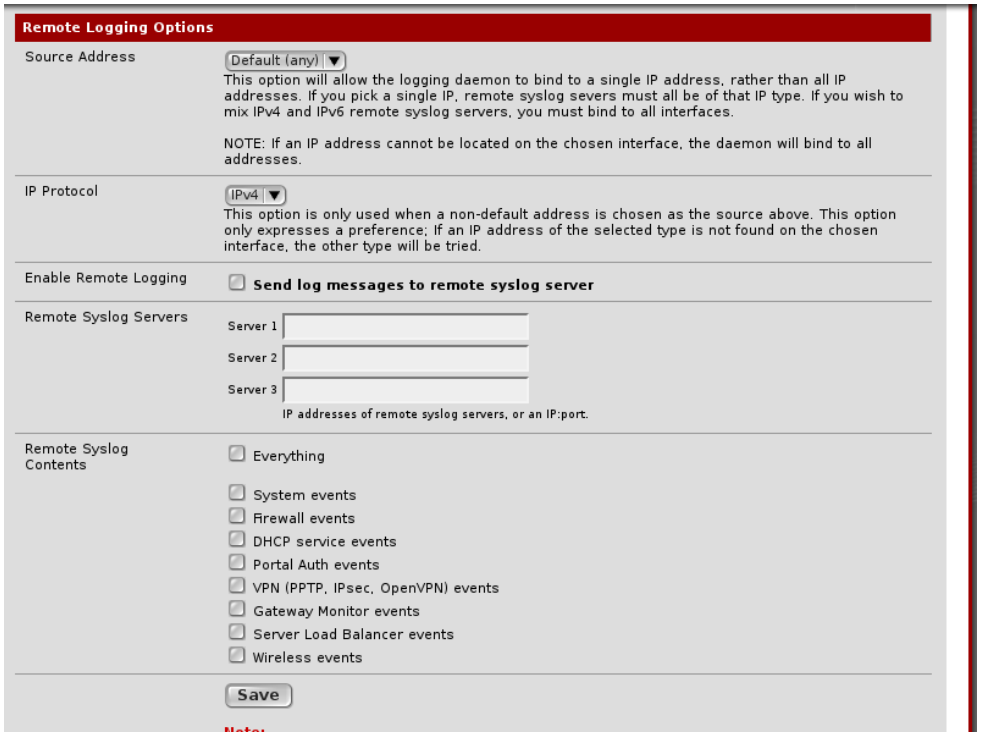
You can setup syslog forwarding, if you have a syslog server.

The firewall will send UDP syslog packets to port 514 – which is fairly standard.

Goto the menu Status -> System logs.

Then click on the ‘Settings’ tab.

Scroll to the bottom to see the settings to send logs to a remote syslog server:



NB. If your syslog server listens on a different port, note that this can be specified after the IP address with a ‘:’.

The use of a sys log service can be very useful for tracking down drops in packets days or weeks later.

The output you'll recive from the syslog server will be something like:

```
Apr 27 00:02:25 angelus.classics.ox.ac.uk filterlog: 46,16777216,,1000000117,em0,match,block,in,4,0x0,,46,38268,0,DF,6,tcp,91,221.229.166.28,163.1
.169.206,56081,22,39,FPA,3685133662:3685133701,555937040,229,,nop;nop;TS
Apr 27 00:02:25 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x0,,112,10050,0,DF,6,tcp,48,81.141.92.141,163.1.
169.239,60033,8192,0,S,1993106255,,8192,,mss;nop;nop;sackOK
Apr 27 00:02:28 angelus.classics.ox.ac.uk filterlog: 47,16777216,,1000000118,em1,match,block,in,4,0x0,,64,0,0,DF,6,tcp,60,163.1.169.206,221.229.16
6.28,22,56081,0,SA,555937039,3685133662,5792,,mss;sackOK;TS;nop;wscale
Apr 27 00:02:28 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29397,0,DF,6,tcp,48,82.5.15.47,163.1.169
.239,49907,8192,0,S,972047577,,8192,,mss;nop;nop;sackOK
Apr 27 00:02:35 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x8,,239,35063,0,none,6,tcp,40,93.174.95.83,163.1
.169.138,50549,389,0,S,3843301624,,1024,,
Apr 27 00:02:35 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29400,0,DF,6,tcp,52,82.5.15.47,163.1.169
.152,49916,8027,0,S,2589359241,,8192,,mss;nop;wscale;nop;nop;sackOK
Apr 27 00:02:38 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29401,0,DF,6,tcp,52,82.5.15.47,163.1.169
.152,49916,8027,0,S,2589359241,,8192,,mss;nop;wscale;nop;nop;sackOK
Apr 27 00:02:42 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29405,0,DF,6,tcp,52,82.5.15.47,163.1.169
.239,49907,8192,0,S,977951847,,8192,,mss;nop;wscale;nop;nop;sackOK
Apr 27 00:02:44 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29406,0,DF,6,tcp,48,82.5.15.47,163.1.169
.152,49916,8027,0,S,2589359241,,8192,,mss;nop;nop;sackOK
Apr 27 00:02:44 angelus.classics.ox.ac.uk filterlog: 5,16777216,,1000000103,em0,match,block,in,4,0x8,,239,42515,0,none,6,tcp,40,93.174.95.83,163.1
.169.116,50549,250,0,S,2850557853,,1024,,
```

Breaking this comma separated data down we have an example packet drop from the firewall:

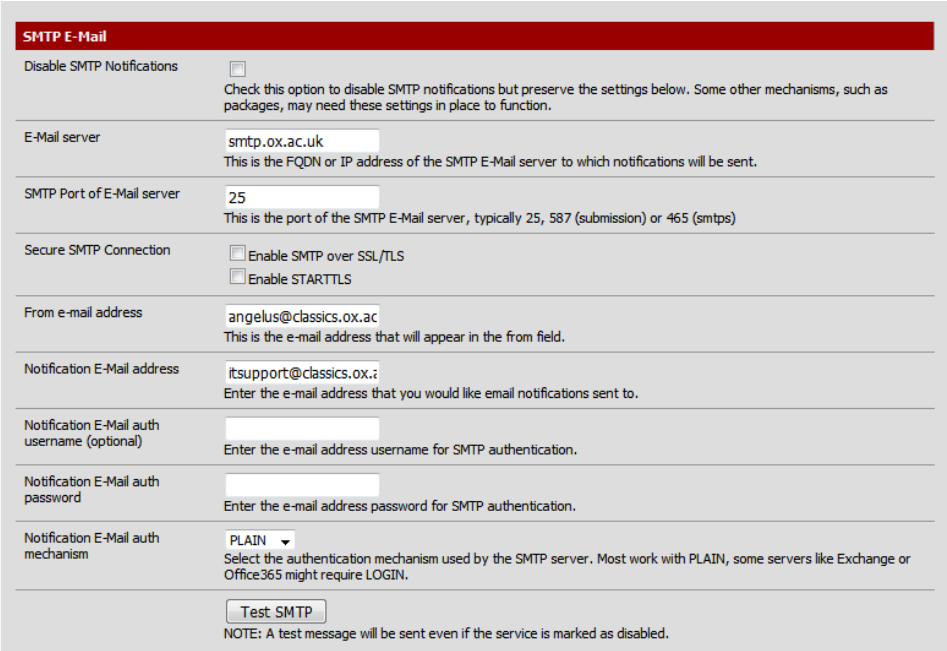
Apr 27 00:02:42 angelus.classics.ox.ac.uk filterlog:
5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29405,0,DF,6,tcp,52,82.5.15.47,16
3.1.169.239,49907,8192,0,S,977951847,,8192,,mss;nop;wscale;nop;nop;sackOK

Data	Type	Comment
Apr 27 00:02:42 angelus.classics.ox.ac.uk filterlog	Date, time and name of firewall host. Also name of service producing the syslog data.	In this case it's a filter/firewall drop that's being logged, although other events will also show up.
5		
16777216		
1000000103		
em0	Interface packet was found on	In this case em0 is the WAN
match	Reason for logging	The packets matched a rule in this case
block	Action the firewall took on the packet	In this case a block. Allowed packets can be logged too at the expense of more data logged.
in	Direction of packet flow.	Inbound to the WAN port from the FroDo/internet
4	IP version (4 or 6)	IPv4
0x0		
114		
29405		
0		
DF		

6	Protocol ID	
tcp	Traffic type	Usually TCP or UDP
52	Packet size in bytes	52 byte packet.
82.5.15.47	Originating IP address	Something on the web
163.1.169.239	Destination IP address	One of our machines.
49907	Port the packet was sent from	
8192	Destination port	
0	Packet **data** length	Size of the data portion of the packet (not the headers)
S	TCP flags (see https://doc.pfsense.org/index.php/What_are_TCP_Flags%3F)	SYN flag set on packet.
977951847		
8192		
mss;wscale;nop;nop;sack;OK		

The format of filter logs is documented on the pfSense site here: https://doc.pfsense.org/index.php/Filter_Log_Format_for_pfSense_2.2

You can also turn on email notifications, see system -> advanced -> notifications



Here we're using the IT Services SMTP server in anonymous mode (only available with the university subnet).

The 'from' email address doesn't actually exist as an account as such, but it is useful to tell you which person or automated system sent the message.

Notification email address is simply who will receive the alerts generated.

What will be sent via email? Not dropped packets, but rather firewall reboots or firmware updates.

Tuning pfsense for your NIC hardware

Refer to the pfSense documentation page (https://doc.pfsense.org/index.php/Tuning_and_Troubleshooting_Network_Cards)

to tune pfSense according to your network card types.

This is worth doing, to ensure your firewall is stable and does have lots of lag or drop packets under load.

You'll may need to use SSH (setup earlier) using the admin user credentials already set. The default text editor is 'VI' – If you don't know VI, then this 'cheat sheet' http://www.lagmonster.org/docs/vi.html should help when creating new config files.