

# Setting up pfSense as a Stateful Bridging Firewall.

## Contents

### Contents

Setting up pfSense as a Stateful Bridging Firewall.....	1
What kind of system these directions will try and help you create.....	1
Selecting your server.....	1
Installing pfSense .....	3
Setting up the basics (IP assignment, etc) .....	6
The first task is interface assignment .....	6
Assigning an IP for web management. ....	8
How to setup bridging mode .....	14
Disable the auto-creation of NAT rules.....	14
Change the WAN and OPT1 interface configuration .....	15
Creating the bridge interface.....	16
Checking the filter options.....	17

---

### What kind 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

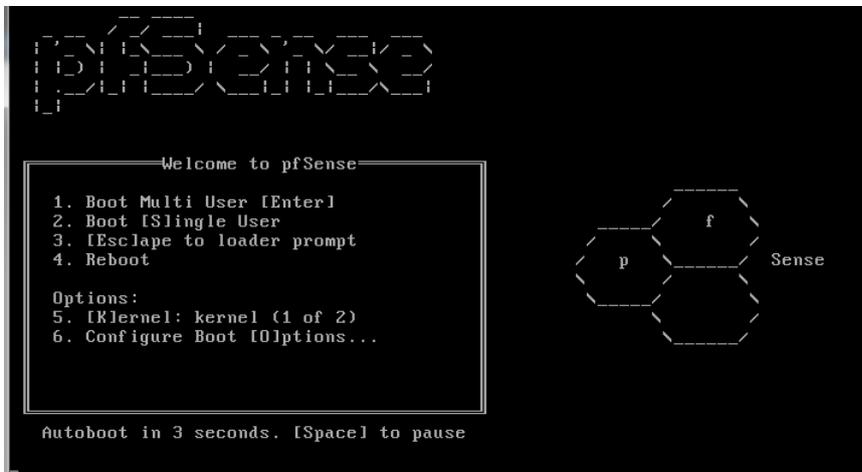
<https://www.pfsense.org/download/mirror.php?section=downloads>

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

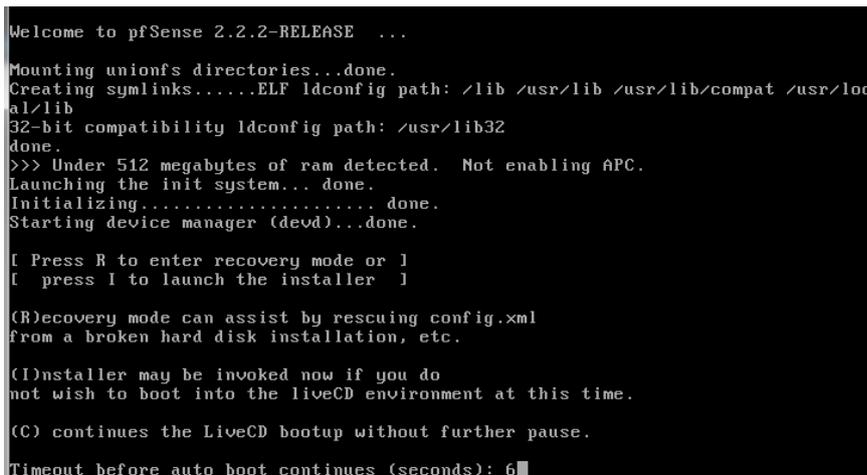
Select the correct 32/64bit version of pfSense to match your server.

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

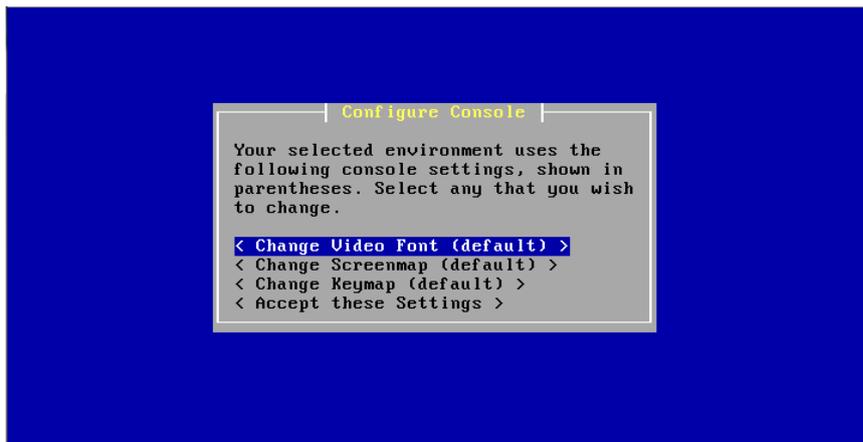
Once you've downloaded the ISO and burnt it to CD, boot your server and you should see:



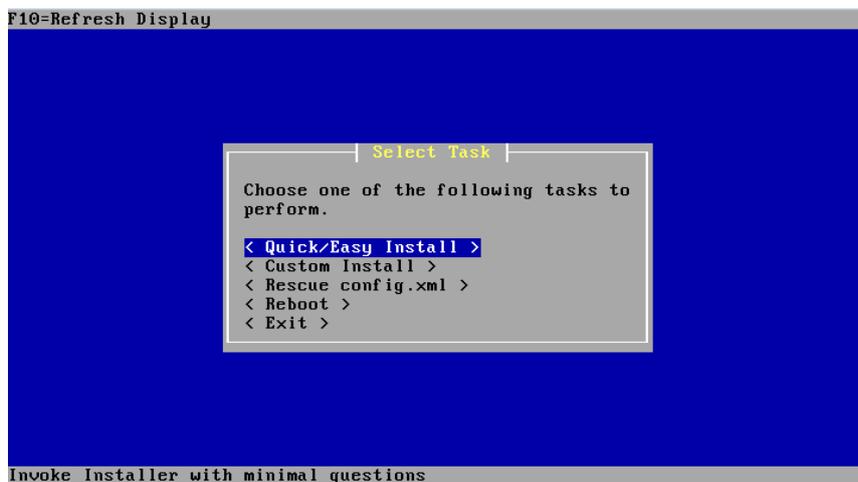
Then you'll get to an options screen which will give you the option to install if you press 'i':



Pressing 'i' gets you to a configure, select 'accept these settings':



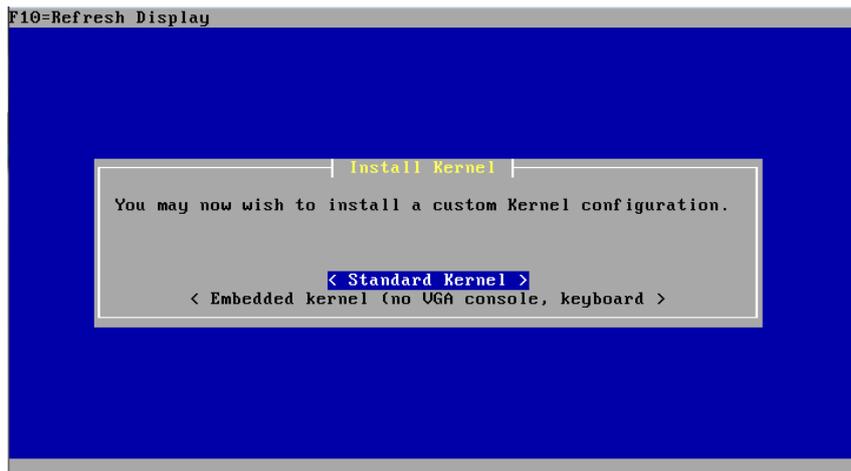
Then select 'Quick/Easy Install':



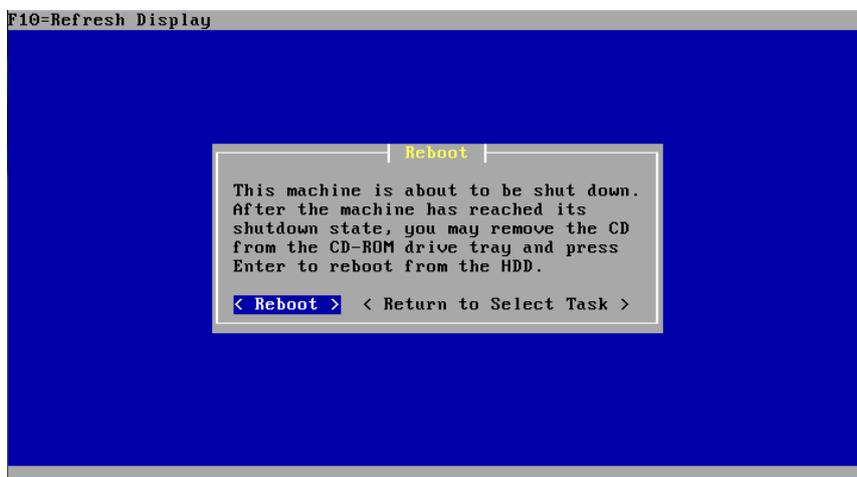
Accept the fact you server's disks will be formatted and the data (if any) will be lost:



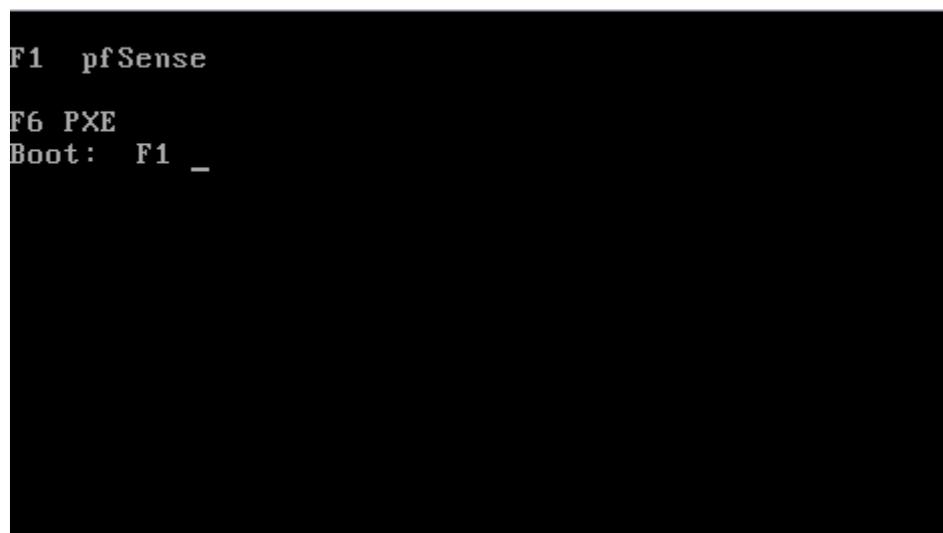
Wait a brief moment as the partitioning occurs, then select 'Standard Kernel':



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

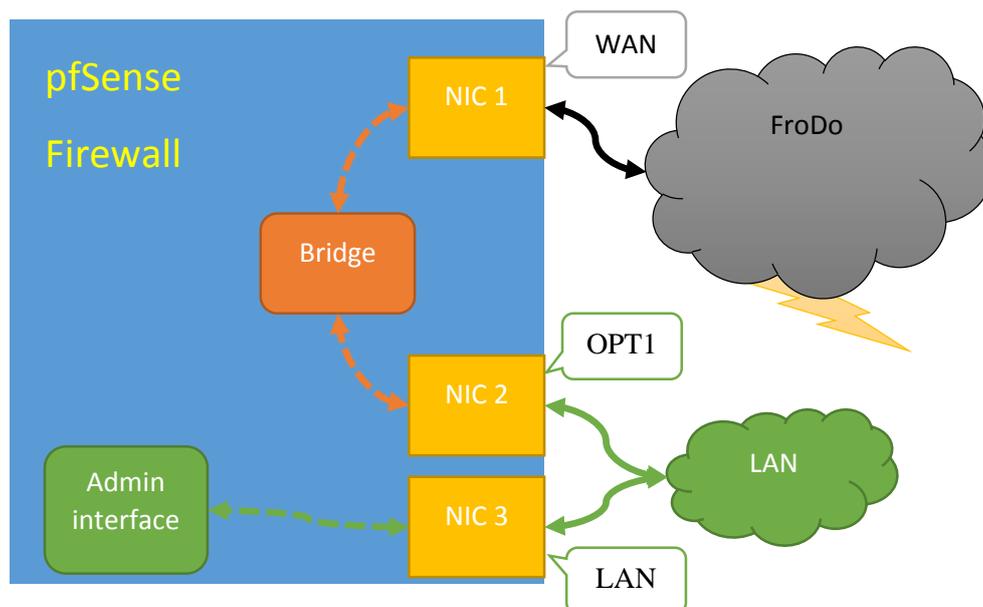
Enter an option: █
```

### 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 accidentally 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:

```
Enter an option: 1

Valid interfaces are:
em0      08:00:27:d8:bd:ac   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em1      08:00:27:77:5c:f7   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em2      08:00:27:50:8e:79 (down) Intel(R) PRO/1000 Legacy Network Connection 1.0.6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]?
```

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

```
Do you want to set up VLANs now [y/n]? n

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection:
```

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).

```

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: a

Connect the WAN interface now and make sure that the link is up.
Then press ENTER to continue.

Detected link-up on interface em0.

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished):

```

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 assignments for you to confirm:

```

The interfaces will be assigned as follows:

WAN   -> em0
LAN   -> em1
OPT1  -> em2

Do you want to proceed [y/n]?

```

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.

```

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
>

```

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 the new LAN IPv4 address. Press <ENTER> for none:
> 163.1.169.77

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 163.1.169.254

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
```

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.

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

The IPv4 LAN address has been set to 163.1.169.77/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://163.1.169.77/

Press <ENTER> to continue.
```

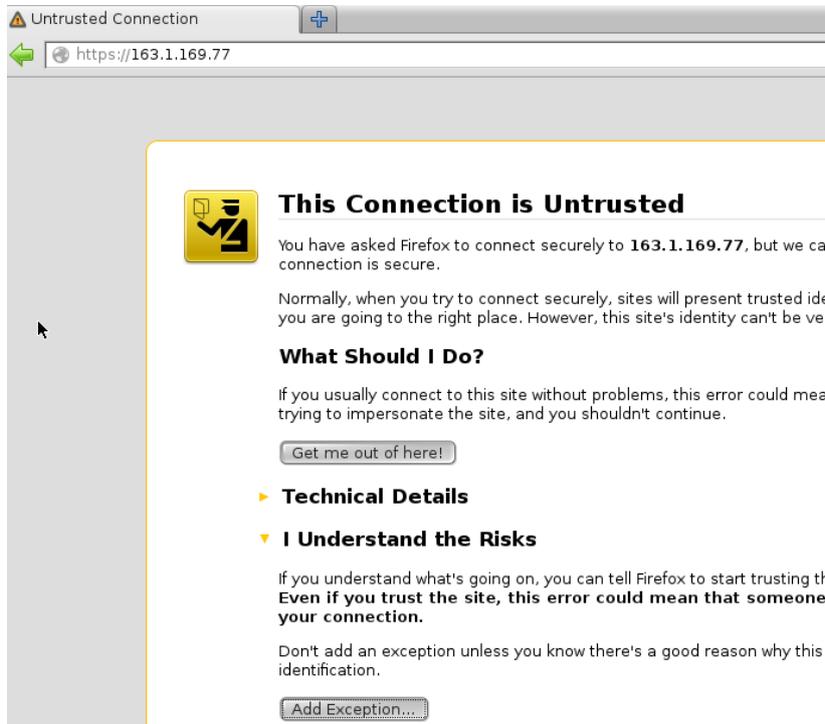
More configuration with a browser.

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

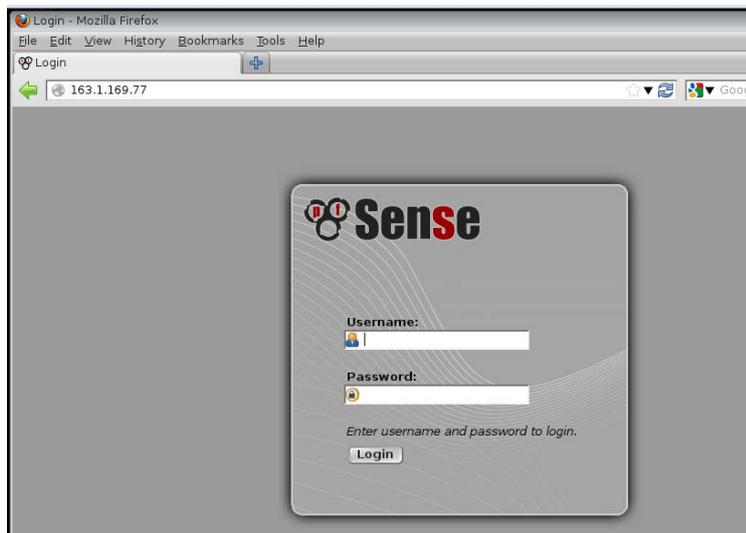
Our first task is to logon and change the admin password.

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:

General Information	
<b>Hostname:</b>	<input type="text" value="medusa"/> EXAMPLE: myserver
<b>Domain:</b>	<input type="text" value="classics.ox.ac.uk"/> EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and use the manually configured DNS servers directly. To use the manually configured DNS servers below for client queries, and enable DNS Query Forwarding after completing the wizard.	
<b>Primary DNS Server:</b>	<input type="text" value="129.67.1.1"/>
<b>Secondary DNS Server:</b>	<input type="text" value="163.1.2.1"/>
<b>Override DNS:</b>	<input type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

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

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

Time Server Information	
<b>Time server hostname:</b>	<input type="text" value="ntp.ox.ac.uk"/> Enter the hostname (FQDN) of the time server.
<b>Timezone:</b>	<input type="text" value="Europe/London"/>

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:

**RFC1918 Networks**

**Block RFC1918 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. Block private networks from entering via WAN

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

**Configure LAN Interface**

**LAN IP Address:**   
Type dhcp if this interface uses DHCP to obtain

**Subnet Mask:**

Finally you can set a password for the firewall:

**Set Admin WebGUI Password**

**Admin Password:**

**Admin Password AGAIN:**

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:

A reload is now in progress. Please wait.  
The wizard will redirect to the next step once the reload is completed.

**Reload in progress**

...

**Congratulations! pfSense is now configured.**  
Please consider contributing back to the project!  
Click [here](#) to purchase services offered by the pfSense team and find other ways to contribute.  
Click [here](#) to continue on to pfSense webConfigurator.

**Wizard completed.**

Done.

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

The screenshot shows a web browser window displaying the pfSense Status Dashboard. The browser's address bar shows the URL `https://163.1.169.77`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Status: Dashboard" and contains two primary panels: "System Information" and "Interfaces".

**System Information**

Name	medusa.classics.ox.ac.uk
Version	2.2.2-RELEASE (amd64) built on Mon Apr 13 20:10:22 CDT 2015 FreeBSD 10.1-RELEASE-p9  Unable to check for updates.
Platform	pfSense
CPU Type	Intel(R) Core(TM) i5-3230M CPU @ 2.60GHz
Uptime	00 Hour 13 Minutes 52 Seconds
Current date/time	Fri Apr 24 13:17:44 BST 2015
DNS server(s)	127.0.0.1 163.1.2.1 129.67.1.1
Last config change	Fri Apr 24 13:17:22 BST 2015
State table size	0% (24/47000) Show states
MBUF	

**Interfaces**

WAN (DHCP)	↑	1000baseT <full-duplex> 0.0.0.0
LAN	↑	1000baseT <full-duplex> 163.1.169.77

## 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](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

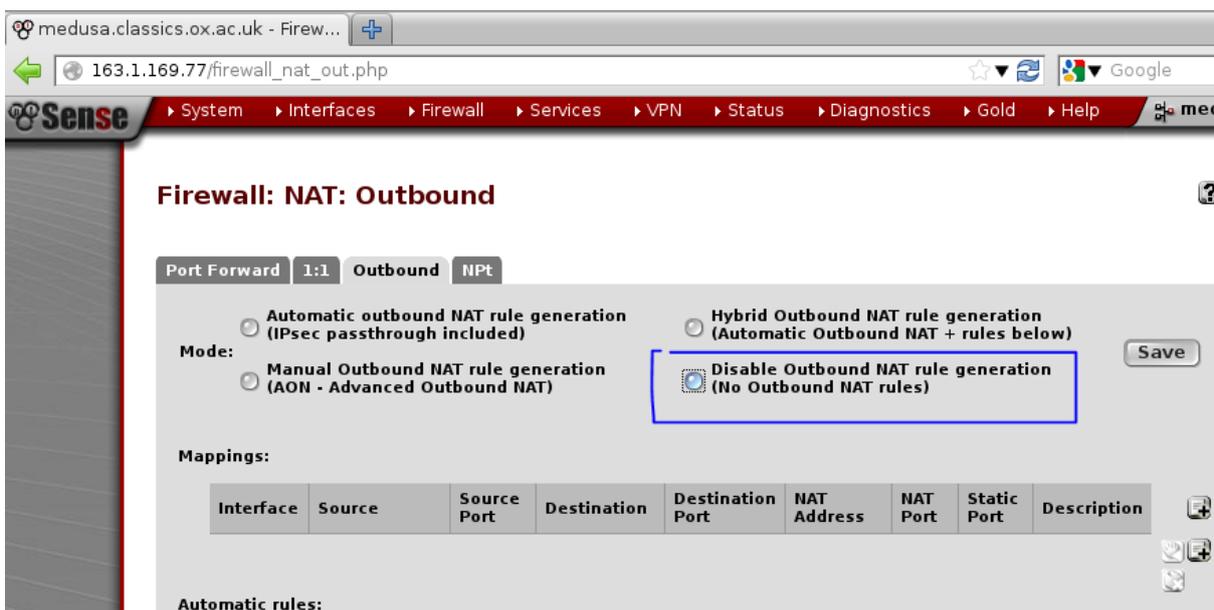
Disable the auto-creation of NAT rules

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:

The screenshot shows the Mikrotik WinBox interface for configuring the OPT1 interface. The breadcrumb navigation at the top reads: System > Interfaces > Firewall > Services > VPN > Status. The main heading is "Interfaces: OPT1". Under the "General configuration" section, the "Enable" checkbox is checked, and the text "Enable Interface" is displayed. The "Description" field contains "OPT1" with a note: "Enter a description (name) for the interface here." Below this, the "IPv4 Configuration Type" and "IPv6 Configuration Type" are both set to "None" via dropdown menus. The "MAC address" field is empty, with a note: "This field can be used to modify ('spooF') the MAC (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx".

Interfaces: OPT1

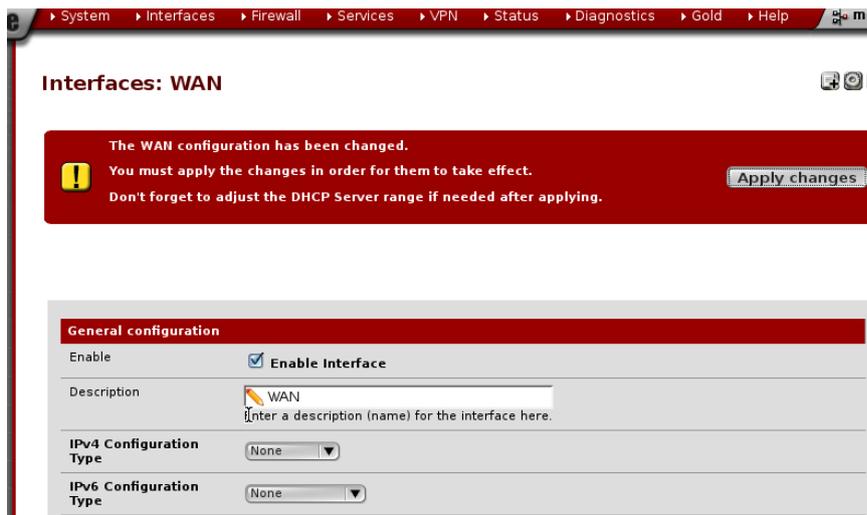


The OPT1 configuration has been changed.  
**!** You must apply the changes in order for them to take effect.  
Don't forget to adjust the DHCP Server range if needed after applying. Apply changes

You'll also need to 'apply changes' made.

Goto the interfaces drop down menu and select WAN.

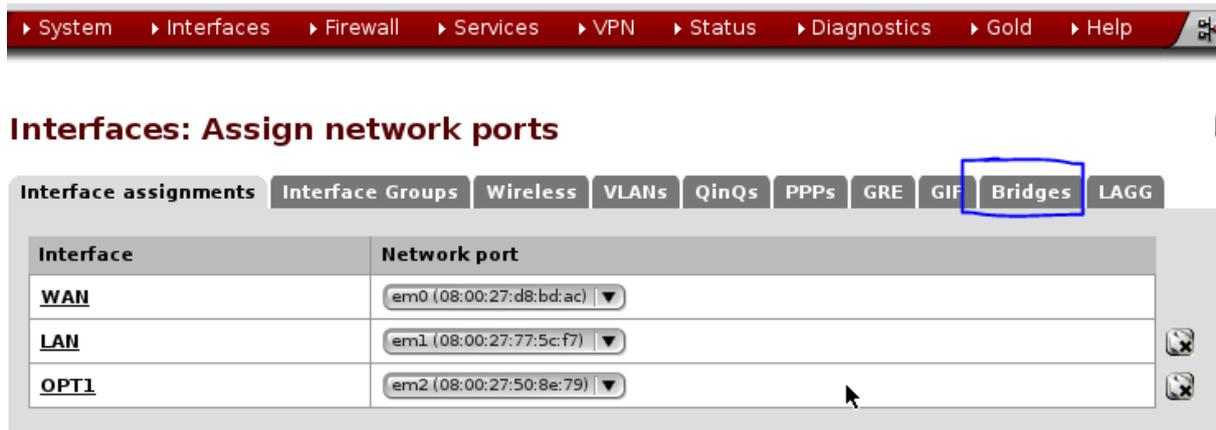
Change the IPv4 and IPv6 configuration types to 'none'



Click save and apply the changes.

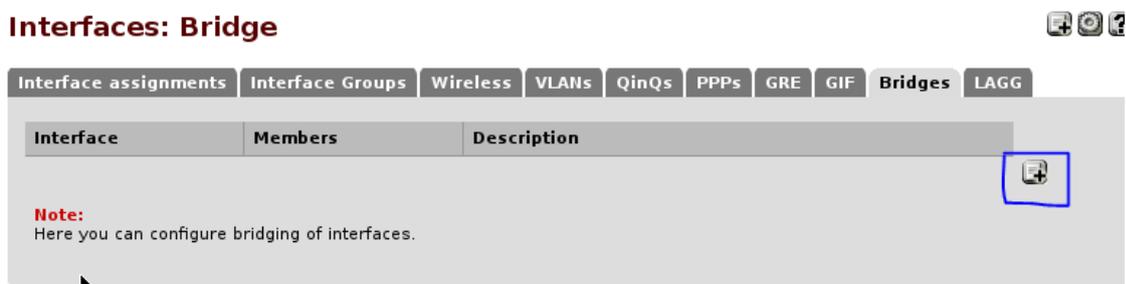
Creating the bridge interface

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



Interfaces that are configured as members of a lagg(4) interface will not be shown.

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:

## Interfaces: Bridge: Edit

**Bridge configuration**

**Member interfaces**  
  
Interfaces participating in the bridge.

**Description**  
 bridge

Click save and you should have a bridging firewall!:

## Interfaces: Bridge



**Interface assignments** **Interface Groups** **Wireless** **VLANs** **QinQs** **PPPs** **GRE** **GIF** **Bridges** **LAGG**

Interface	Members	Description
BRIDGE0	WAN, OPT1	bridge


**Note:**  
Here you can configure bridging of interfaces.

### 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:

Secure Shell	
Secure Shell Server	<input checked="" type="checkbox"/> <b>Enable Secure Shell</b>
Authentication Method	<input type="checkbox"/> <b>Disable password login for Secure Shell (RSA/DSA key only)</b> When enabled, authorized keys need to be configured for each user that has been granted secure shell access.
SSH port	<input type="text"/> Note: Leave this blank for the default of 22.

Save those changes.

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

Disable reply-to	<input checked="" type="checkbox"/> <b>Disable reply-to on WAN rules</b> With Multi-WAN you generally want to ensure traffic leaves the same interface it arrives on, hence reply-to is added automatically by default. When using bridging, you must disable this behavior if the WAN gateway IP is different from the gateway IP of the hosts behind the bridged interface.
------------------	--

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

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Gold > Help

Admin Access | **Firewall / NAT** | Networking | Miscellaneous | System Tunables | Notifications

**NOTE:** The options on this page are intended for use by advanced users only.

### Firewall Advanced

IP Do-Not-Fragment compatibility	<input checked="" type="checkbox"/> <b>Clear invalid DF bits instead of dropping the packets</b> This allows for communications with hosts that generate fragmented packets with the don't fragment (DF) bit set. Linux NFS is known to do this. This will cause the filter to not drop such packets but instead clear the don't fragment bit.
IP Random id generation	<input type="checkbox"/> <b>Insert a stronger id into IP header of packets passing through the filter.</b> Replaces the IP identification field of packets with random values to compensate for operating systems that use predictable values. This option only applies to packets that are not fragmented after the optional packet reassembly.
Firewall Optimization Options	<input type="text" value="conservative"/> tries to avoid dropping any legitimate idle connections at the expense of increased memory usage and CPU utilization. Select the type of state table optimization to use
Disable Firewall	<input type="checkbox"/> <b>Disable all packet filtering.</b> Note: This converts pfSense into a routing only platform! Note: This will also turn off NAT! If you only want to disable NAT, and not firewall rules, visit the <a href="#">Outbound NAT</a> page.
Disable Firewall Scrub	<input checked="" type="checkbox"/> <b>Disables the PF scrubbing option which can sometimes interfere with NFS and PPTP traffic.</b>

Click save.

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

**Network Interfaces**

Device polling  **Enable device polling**  
 Device polling is a technique that lets the system periodically poll network devices for new data instead of relying on interrupts. This prevents your webConfigurator, SSH, etc. from being inaccessible due to interrupt floods when under extreme load. Generally this is not recommended. Not all NICs support polling; see the pfSense homepage for a list of supported cards.

Hardware Checksum Offloading  **Disable hardware checksum offload**  
 Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs.  
**Note:** This will take effect after you reboot the machine or re-configure each interface.

Hardware TCP Segmentation Offloading  **Disable hardware TCP segmentation offload**  
 Checking this option will disable hardware TCP segmentation offloading (TSO, TSO4, TSO6). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs.  
**Note:** This will take effect after you reboot the machine or re-configure each interface.

Hardware Large Receive Offloading  **Disable hardware large receive offload**  
 Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs.  
**Note:** This will take effect after you reboot the machine or re-configure each interface.

ARP Handling  **Suppress ARP messages**  
 This option will suppress ARP log messages when multiple interfaces reside on the same broadcast domain

Make sure you save again...

Adding a third DNS server – System -> General setup

Enter the 3<sup>rd</sup> IT services DNS resolver:

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Gold

**System: General Setup**

**System**

**Hostname** medusa  
 Name of the firewall host, without domain part  
 e.g. *firewall*

**Domain** classics.ox.ac.uk  
 Do not use 'local' as a domain name. It will cause local hosts running mDNS (ava to be unable to resolve local hosts not running mDNS.  
 e.g. *mycorp.com, home, office, private, etc.*

**DNS servers**

DNS Server	Use gateway
129.67.1.1	none
163.1.2.1	none
129.67.1.180	none
	none

Enter IP addresses to be used by the system for DNS resolution. These are also

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:

### Firewall: Rules: Edit

Edit Firewall rule	
<b>Action</b>	<input type="text" value="Pass"/> Choose what to do with packets that match the criteria specified. Hint: the difference between block and reject is that with reject (unreachable for UDP) is returned to the sender, whereas with block, either case, the original packet is discarded.
<b>Disabled</b>	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the firewall.
<b>Interface</b>	<input type="text" value="OPT1"/> Choose which interface packets must be sourced on to match this rule.
<b>TCP/IP Version</b>	<input type="text" value="IPv4"/> <b>Select the Internet Protocol version.</b>
<b>Protocol</b>	<input type="text" value="any"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
<b>Source</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="127"/>
<b>Destination</b>	<input type="checkbox"/> <b>not</b>

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

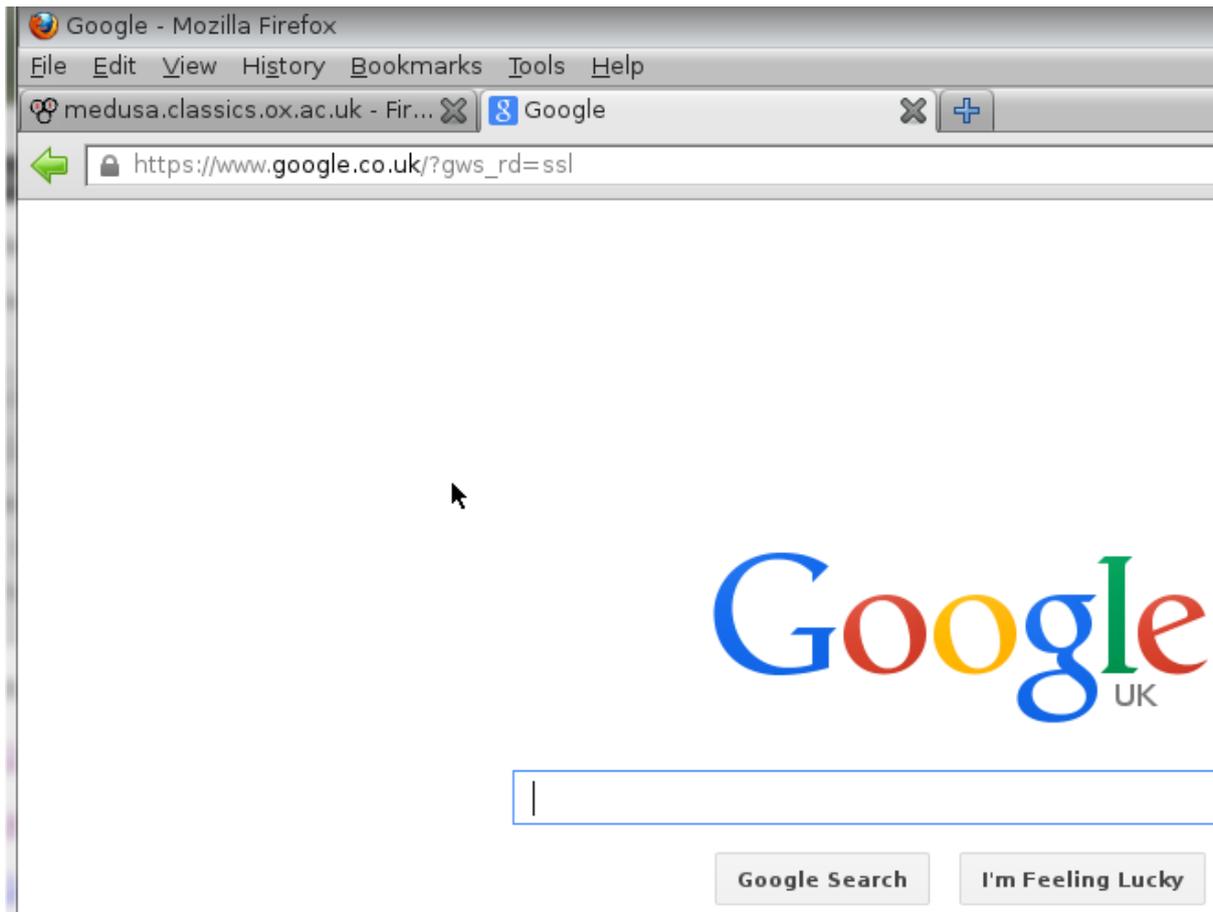
This will allow all IPv4 traffic out from our LAN via the OPT1 interface (if you want to be more restrictive, you can create individual rules for outbound traffic on the OPT1 interface).

Update the description and save:

<b>Description</b>	<input type="text" value="Default allow OPT1 to any rule"/> You may enter a description here for your reference.
--------------------	---

Finally 'Apply changes'.

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



## Setting up your own rules.

### Aliases

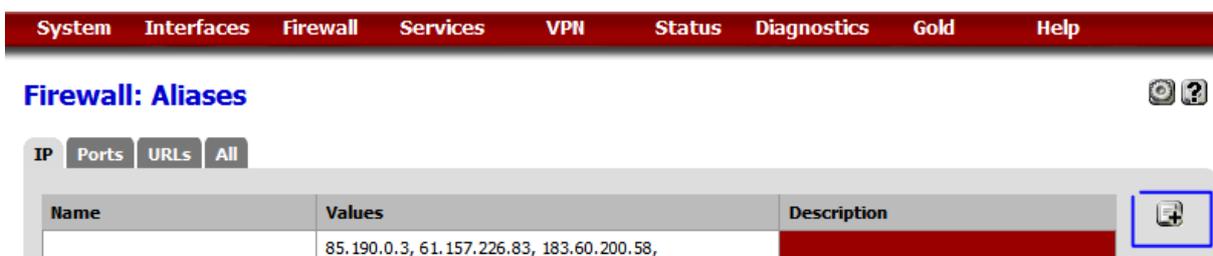
Firewall rules work best when using aliases.

You can use an Alias 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
- ...

## Firewall: Aliases: Edit

**Alias Edit**

**Name**   
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description**   
You may enter a description here for your reference (not parsed).

**Type**

**Host(s)**

Enter as many hosts as you would like. Hosts must be specified by their IP address or fully qual (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned used. You may also enter an IP range such as 192.168.1.1-192.168.1.10 or a small subnet such and a list of individual IP addresses will be generated.

IP or FQDN	Description
163.1.169.42	Classics example machine

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

The '+' is clicked on to enter IPs/FQDNs and clicked on again to enter another IP/FQDN.

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

System Interfaces Firewall Services VPN Status Dia

## Firewall: Rules: Edit

### Edit Firewall rule

Action	<input type="text" value="Pass"/> <p>Choose what to do with packets that match the criteria specified by this rule. Hint: the difference between block and reject is that with reject, a packet is returned to the sender, whereas with block the packet is dropped.</p>
Disabled	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
Interface	<input type="text" value="WAN"/> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<input type="text" value="IPv4"/> <b>Select the Internet Protocol version that this rule should match.</b>
Protocol	<input type="text" value="TCP"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match.
	Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="127"/>
	<input type="button" value="Advanced"/> - Show source port range

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

Destination port range	from: <input type="text" value="(other)"/> <input type="text" value=""/> to: <input type="text" value="(other)"/> <input type="text" value=""/> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port.</p>
------------------------	--

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:

Source	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match.
	Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="127"/>
	<input type="button" value="Advanced"/> - Show source port range

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

Hint: in most cases, you should specify *TCP* here.

**Source**

**not**  
Use this option to invert the sense of the match.

Type:

Address:  /

---

**Source port range**

from:

to:

Specify the source port or port range for this rule. **This is usually *random* and almost never equal to the destination port range (and should usually be "any")**.  
Hint: you can leave the 'to' field empty if you only want to filter a single port.

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:

### Firewall: Rules



**!** The settings have been applied. The firewall rules are now reloading in the background. You can also monitor the reload progress Close

Floating **WAN** LAN OPT1

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/>	IPv4 UDP	163.1.169.254	*	*	68	*	none		DHCP lease

pass     match     block     reject     log  
 pass (disabled)     match (disabled)     block (disabled)     reject (disabled)     log (disabled)

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

<input checked="" type="checkbox"/>	IPv4 TCP/UDP	Oxford_DNS_Forwarders	*	163.1.169.55	53 (DNS)	*	none		DNS requests to AD server 1
-------------------------------------	--------------	-----------------------	---	--------------	----------	---	------	--	-----------------------------

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:

The screenshot shows the 'Remote Logging Options' configuration page. It includes the following sections:

- Source Address:** A dropdown menu set to 'Default (any)'. Below it is a note: 'This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If you pick a single IP, remote syslog servers must all be of that IP type. If you wish to mix IPv4 and IPv6 remote syslog servers, you must bind to all interfaces.' A further note states: 'NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.'
- IP Protocol:** A dropdown menu set to 'IPv4'. Below it is a note: 'This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.'
- Enable Remote Logging:** A checkbox labeled 'Send log messages to remote syslog server' which is currently unchecked.
- Remote Syslog Servers:** Three input fields labeled 'Server 1', 'Server 2', and 'Server 3'. Below them is the text: 'IP addresses of remote syslog servers, or an IP:port.'
- Remote Syslog Contents:** A list of checkboxes for logging content: 'Everything' (unchecked), 'System events' (unchecked), 'Firewall events' (unchecked), 'DHCP service events' (unchecked), 'Portal Auth events' (unchecked), 'VPN (PPTP, IPsec, OpenVPN) events' (unchecked), 'Gateway Monitor events' (unchecked), 'Server Load Balancer events' (unchecked), and 'Wireless events' (unchecked).
- Save:** A button at the bottom of the form.

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 receive from the syslog server will be something like:

```
Apr 27 00:02:25 angelus.classics.ox.ac.uk filterlog: 46,16777216,,100000117,em0,match,block,in,4,0x0,,46,38268,0,DF,6,tcp,31,221.229.166.28,163.1.169.206,56081,22,39,FPA,3685133662:3685133701,555937040,229,,nop;nop;TS
Apr 27 00:02:25 angelus.classics.ox.ac.uk filterlog: 5,16777216,,100000103,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,,100000118,em1,match,block,in,4,0x0,,64,0,0,DF,6,tcp,60,163.1.169.206,221.229.166.28,22,56081,0,SA,555937039,3685133662,5792,,mss;sackOK;TS;nop;wscale
Apr 27 00:02:28 angelus.classics.ox.ac.uk filterlog: 5,16777216,,100000103,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,,100000103,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,,100000103,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,,100000103,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,,100000103,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,,100000103,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,,100000103,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:

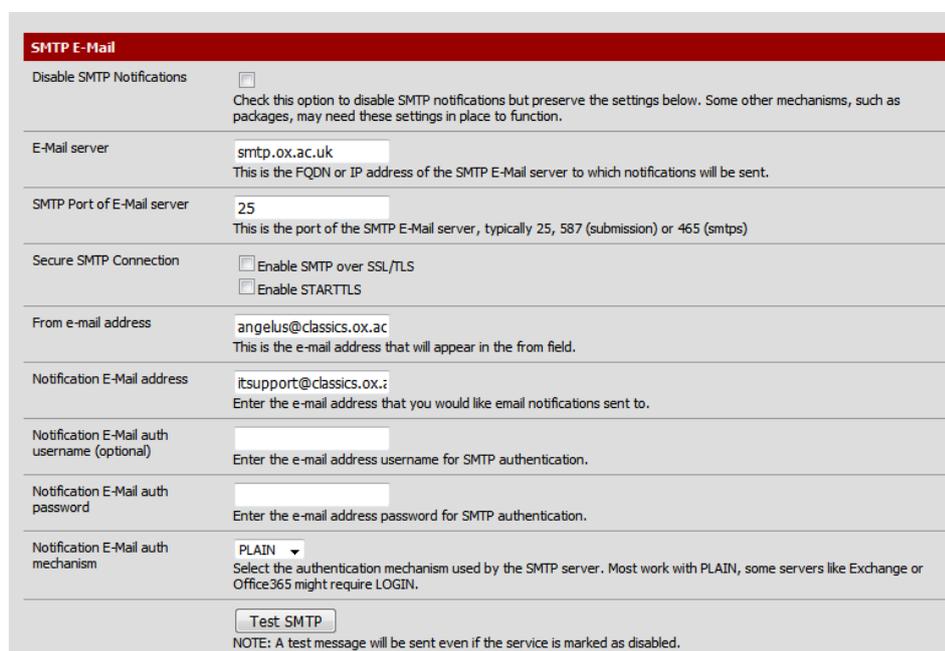
5,16777216,,1000000103,em0,match,block,in,4,0x0,,114,29405,0,DF,6,tcp,52,82.5.15.47,16  
3.1.169.239,49907,8192,0,S,977951847,,8192,,mss;nop;wscale;nop;nop;sackOK

Data	Type	Comment
Apr 27 00:02:42 angelus.classics.ox.ac.u k filterlog	Date, time and name of firewall host. Also name of service producing the syslog data.	In this case it's a filter/firewa ll 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/inter net
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 <b>data</b> length	Size of the data portion of the packet (not the headers)
S	TCP flags (see <a href="https://doc.pfsense.org/index.php/What_are_TCP_Flags%3F">https://doc.pfsense.org/index.php/What_are_TCP_Flags%3F</a> )	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](https://doc.pfsense.org/index.php/Filter_Log_Format_for_pfSense_2.2)

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



SMTP E-Mail	
Disable SMTP Notifications	<input type="checkbox"/> Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.
E-Mail server	smtp.ox.ac.uk This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.
SMTP Port of E-Mail server	25 This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps)
Secure SMTP Connection	<input type="checkbox"/> Enable SMTP over SSL/TLS <input type="checkbox"/> Enable STARTTLS
From e-mail address	angelus@classics.ox.ac This is the e-mail address that will appear in the from field.
Notification E-Mail address	itsupport@classics.ox.ac Enter the e-mail address that you would like email notifications sent to.
Notification E-Mail auth username (optional)	<input type="text"/> Enter the e-mail address username for SMTP authentication.
Notification E-Mail auth password	<input type="password"/> Enter the e-mail address password for SMTP authentication.
Notification E-Mail auth mechanism	PLAIN Select the authentication mechanism used by the SMTP server. Most work with PLAIN, some servers like Exchange or Office365 might require LOGIN.
<input type="button" value="Test SMTP"/> NOTE: A test message will be sent even if the service is marked as disabled.	

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](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 not 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.