Setting up pfSense as a Stateful Bridging Firewall.

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 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:

![pfSense options screen]

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

![pfSense installation options]

Diggory Gray Faculty of Classics 27/4/2015
Pressing ‘i’ gets you to a configure, select ‘accept these settings’:

Then select ‘Quick/Easy Install’:

Accept the fact your 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:

```
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-PM
8) Shell
```

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:

```
Valid interfaces are:
em0  08:00:27:d0:bd:ac  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
em1  08:00:27:71:5c:ff  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
em2  08:00:27:50:8e:79  (down) Intel(R) PRO/1000 Legacy Network Connection 1.0.
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 [yn]?
```

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 [yn]? 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).
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:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Assigned NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN</td>
<td>em0</td>
</tr>
<tr>
<td>LAN</td>
<td>em1</td>
</tr>
<tr>
<td>OPT1</td>
<td>em2</td>
</tr>
</tbody>
</table>

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 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 = 0

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 DHCP...
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...
DHCP...

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):

![Untrusted Connection]

**This Connection is Untrusted**

You have asked Firefox to connect securely to 163.1.169.77, but we can't verify that this connection is secure.

Normally, when you try to connect securely, sites will present trusted info to you, showing that you are going to the right place. However, this site’s identity can't be verified.

**What Should I Do?**

If you usually trust this site without problems, this error could mean that you are trying to impersonate the site, and you shouldn’t continue.

- Get me out of here!

**Technical Details**

- I Understand the Risks

If you understand what’s going on, you can tell Firefox to trust this site even if you trust the site, this error could mean that someone is trying to impersonate the site.

Don’t add an exception unless you know there’s a good reason why this site’s identity is correct.

- Add Exception...

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.

![Sense Login]

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:

<table>
<thead>
<tr>
<th>General Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Domain:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

NB. Uncheck the ‘Override DNS’ box at the bottom.

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

<table>
<thead>
<tr>
<th>Time Server Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time server hostname:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Timezone:</strong></td>
</tr>
</tbody>
</table>

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:

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):
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.

Diggory Gray Faculty of Classics 27/4/2015
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:

**Interfaces: Bridge: Edit**

<table>
<thead>
<tr>
<th>Member interfaces</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>bridge</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.link.bridge.pli_onlyip</td>
<td>Only pass IP packets when pf is enabled 0</td>
</tr>
<tr>
<td>net.link.bridge.pli_member</td>
<td>Packet filter on the member interface 1</td>
</tr>
<tr>
<td>net.link.bridge.pli_bridge</td>
<td>Packet filter on the bridge interface 0</td>
</tr>
</tbody>
</table>

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
Enable Secure Shell

Authentication Method
☐ Disable password login for Secure Shell (RSA/DSA key only)
When enabled, authorized keys need to be configured for each user that has been granted secure shell access.

SSH port

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

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:

```
Firewall Advanced

☐ Clear invalid DF bits instead of dropping the packets
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.

☐ Insert a stronger id into IP header of packets passing through the filter.
Replaces the 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

☐ [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 all packet filtering.
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 Outbound NAT page.

☐ Disable Firewall Scrub
Disables the PF scrubbing option which can sometimes interfere with NFS and PPTP traffic.
```

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:

```
System: General Setup
```

```
System

Hostname

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

Domain

classics.ox.ac.uk

D DNS servers

<table>
<thead>
<tr>
<th>DNS Server</th>
<th>Use gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>129.67.1.1</td>
<td>none</td>
</tr>
<tr>
<td>183.1.2.1</td>
<td>none</td>
</tr>
<tr>
<td>129.67.1.180</td>
<td>none</td>
</tr>
</tbody>
</table>

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

Save your changes, as usual.

Diggory Gray

Faculty of Classics

27/4/2015
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**

<table>
<thead>
<tr>
<th>Action</th>
<th>Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Choose what to do with packets that match the criteria.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disabled</th>
<th>Disable this rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set this option to disable this rule without removing it from the configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>OPT1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose which interface packets must be sourced on to match the criteria.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP/IP Version</th>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the Internet Protocol version.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>any</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose which IP protocol this rule should match.</td>
<td>Hint: in most cases, you should specify TCP here.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>any</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this option to invert the sense of the match.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
<th>not</th>
</tr>
</thead>
<tbody>
<tr>
<td>You may enter a description here for your reference.</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Description</th>
<th>Default allow OPT1 to any rule</th>
</tr>
</thead>
</table>

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):

<table>
<thead>
<tr>
<th>IP</th>
<th>Ports</th>
<th>URLs</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>85.190.0.3, 61.157.226.63, 183.68.200.58,</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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/FQDN.

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:

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.

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:

![DHCP firewall rule](image)

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**

![DNS firewall rules](image)

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 syslog service can be very useful for tracking down drops in packets days or weeks later.

Diggory Gray Faculty of Classics 27/4/2015
The output you'll receive from the syslog server will be something like:
Breaking this comma separated data down we have an example packet drop from the firewall:

<table>
<thead>
<tr>
<th>Data</th>
<th>Type</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 27 00:02:42 angelus.classics.ox.ac.uk filterlog</td>
<td>Date, time and name of firewall host. Also name of service producing the syslog data.</td>
<td>In this case it’s a filter/firewall drop that’s being logged, although other events will also show up.</td>
</tr>
<tr>
<td>5</td>
<td>Interface packet was found on</td>
<td>In this case em0 is the WAN</td>
</tr>
<tr>
<td>16777216</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000000103</td>
<td></td>
<td></td>
</tr>
<tr>
<td>em0</td>
<td>Reason for logging</td>
<td>The packets matched a rule in this case</td>
</tr>
<tr>
<td>match</td>
<td></td>
<td></td>
</tr>
<tr>
<td>block</td>
<td>Action the firewall took on the packet</td>
<td>In this case a block. Allowed packets can be logged too at the expense of more data logged.</td>
</tr>
<tr>
<td>in</td>
<td>Direction of packet flow.</td>
<td>Inbound to the WAN port from the FroDo/Internet</td>
</tr>
<tr>
<td>4</td>
<td>IP version (4 or 6)</td>
<td>IPv4</td>
</tr>
<tr>
<td>0x0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>114</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29405</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DF</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protocol ID</td>
<td>Traffic type</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>tcp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Packet size in bytes</td>
<td>52 byte packet.</td>
</tr>
<tr>
<td>82.5.15.47</td>
<td>Originating IP address</td>
<td>Something on the web</td>
</tr>
<tr>
<td>163.1.169.239</td>
<td>Destination IP address</td>
<td>One of our machines.</td>
</tr>
<tr>
<td>49907</td>
<td>Port the packet was sent from</td>
<td></td>
</tr>
<tr>
<td>8192</td>
<td>Destination port</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Packet <strong>data</strong> length</td>
<td>Size of the data portion of the packet (not the headers)</td>
</tr>
<tr>
<td>S</td>
<td>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>)</td>
<td>SYN flag set on packet.</td>
</tr>
<tr>
<td>977951847</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8192</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mss;wscale;nop;nop;sack;OK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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.