ALEPH OBJECTS®
INCORPORATED

FIREWALL

Aleph Objects Firewall

by Aleph Objects, Inc.

Published by Aleph Objects, Inc., 626 West 66th Street, Loveland, Colorado, 80538 USA.

For more information, call +1-970-377-1111 or visit www.alephobjects.com.

20160904

Contents

List of Figures

List of Listings

Introduction

Aleph Objects Network

This document at present is a rough collection of notes of different hardware and software evalutated for Aleph Objects' network. The goal is to build a network out of routers and switches using as much Free Software as possible.

pfSense

Firewall.

Figure 1.1: pfSense Website

1.1 Overview

Aleph Objects has recently deployed pfSense firewalls, replacing OpenBSD.

pfSense — "Free, open source customized distribution of FreeBSD specifically tailored for use as a firewall and router that is entirely managed via web interface."

pfSense was selected as Aleph Objects core router/firewall for backbone connections.

1.2 Initial Configuration Outline

These are the the initial configuration steps for a pfSense firewall. Here is an overview of the steps:

1. Make serial connection to pfSense firewall, and do basic initial setup.
2. Connect via ethernet to pfSense firewall with web browser.
3. Do more initial setup.

4. Connect pfSense router to Internet.
5. Update router.
6. Install new packages.
7. Configure packages.
8. Backup & reboot.

1.2.1 Setup pfSense Hardware

The following pfSense hardware has been tested:

- SG-2220 — Two 1Gb ethernet ports, dual core 1.7GHz, 2GB RAM, 60GB SSD, single 100-240V power supply, fanless.
- SG-2440 — Four 1Gb ethernet ports, dual core 1.7GHz, 4GB RAM, 128GB SSD, single 100-240V power supply, fanless.
- SG-4860 — Six 1Gb ethernet ports, quad core 2.4GHz, 8GB RAM, 128GB SSD, single 100-240V power supply, fanless.
- XG-2758 — High availability, ten 1Gb ethernet, two 10Gb SFP+ modules, eight core 2.4GHz, 16GB RAM 120GB RAID SSD, single 90 264V power supply, fans, 1U rackmount.

Follow these steps to get the hardware set up to configure the pfSense router.

1. Leave the power off for now.
2. Leave the WAN port unplugged for now.
3. Plug the pfSense provided USB cable into the Console port on the firewall and the USB port of your Debian workstation.
4. Plug in the LAN ethernet port into the local LAN switch.

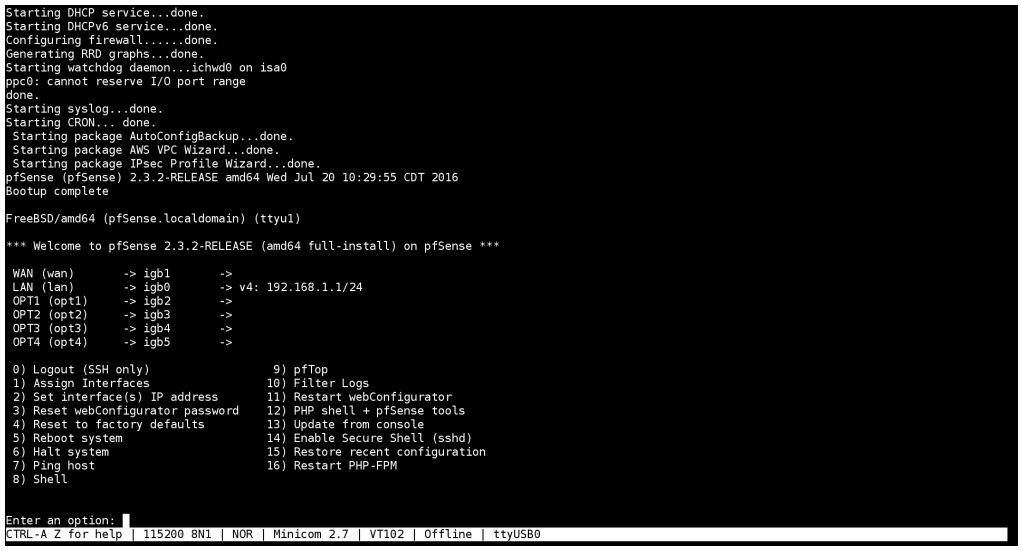

Figure 1.2: pfSense Console

1.2.2 Setup via Serial Connection

With the hardware all plugged in, connect with minicom and do some initial configuration via the USB port. Note, it is possible to start configuration by going to https://192.168.1.1 if you set an IP address on your Debian workstation to an address in that subnet. But you won't be able to see all the bootup messages and it will make debugging/controlling the router more difficult. With the serial connection, you can see the bootloader etc.

1. Find where the USB device connected, by running `dmesg -T` on your Debian workstation. Look for a line with USB0, USB1, etc. in it, such as:

```
usb 1-6: cp210x converter now attached to ttyUSB0
```

2. Run `minicom` on your Debian workstation to connect to the router, using the USB device from above.

```
sudo minicom -D /dev/ttyUSB0
```

Figure 1.3: pfSense Minicom Settings

3. The connection settings are 115200 baud, 8N1, no hardware flow control, no software flow control. Note, hardware flow control is on by default and may prevent you from entering text into the console. To change these settings in minicom, hit `ctrl-a` then the letter `o`. In the menu, with the arrow keys, select `Serial port setup`.

4. Plug in power to the pfSense router, and watch it boot up in minicom. It takes 1 minute, 20 seconds for a SG-4860 to cold boot with a default configuration.

5. In the pfSense menu, select `1) Assign Interfaces`.

```
*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense
 ↪  ***

 WAN (wan)       -> igb1       ->
 LAN (lan)       -> igb0       -> v4: 192.168.1.1/24
 OPT1 (opt1)     -> igb2       ->
 OPT2 (opt2)     -> igb3       ->
 OPT3 (opt3)     -> igb4       ->
 OPT4 (opt4)     -> igb5       ->

 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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: 1
```

```
Valid interfaces are:

igb0   00:08:a2:00:00:00   (up) Intel(R) PRO/1000 Network Connection,
 ↪  Version -
igb1   00:08:a2:00:00:01 (down) Intel(R) PRO/1000 Network Connection,
 ↪  Version -
igb2   00:08:a2:00:00:02 (down) Intel(R) PRO/1000 Network Connection,
 ↪  Version -
igb3   00:08:a2:00:00:03 (down) Intel(R) PRO/1000 Network Connection,
 ↪  Version -
igb4   00:08:a2:00:00:04 (down) Intel(R) PRO/1000 Network Connection,
 ↪  Version -
igb5   00:08:a2:00:00:05 (down) Intel(R) PRO/1000 Network Connection,
 ↪  Version -

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is
 ↪  typical to
say no here and use the webConfigurator to configure VLANs later, if
 ↪  required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(igb0 igb1 igb2 igb3 igb4 igb5 or a): igb1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(igb0 igb2 igb3 igb4 igb5 a or nothing if finished): igb0

Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection
(igb2 igb3 igb4 igb5 a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> igb1
LAN  -> igb0

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

6. Note the MAC address for the LAN interface.
7. Copy MAC address to main DHCP/DNS server, and reserve IP address.

8. Set DHCP for WAN, disable IPv6. This is assuming the WAN is on an interface with DHCP (e.g. cable modem). If it is statically set, set the address here.

```
Enter an option: 2

Available interfaces:

1 - WAN (igb1 - dhcp, dhcp6)
2 - LAN (igb0 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

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

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

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

The IPv4 WAN address has been set to dhcp

Press <ENTER> to continue.
```

9. Set static IP for LAN, using 10.72.9.254/24 as an example. Do not set an IPv6 address. Don't enter a gateway. Don't enable DHCP server (for now, at least).

```
Enter an option: 2

Available interfaces:

1 - WAN (igb1 - dhcp)
2 - LAN (igb0)

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.72.9.254

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:
>

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

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

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 10.72.9.254/24
You can now access the webConfigurator by opening the following URL
 ↪   in your web browser:
                https://10.72.9.254/

Press <ENTER> to continue.
```

1.2.3 Initial Wizard Setup via Web Browser

1. If needed, set IP address on Debian workstation that is in the same subnet as new firewall. If you have two ethernet interfaces, and the new firewall is plugged into the second ethernet interface, depending on the interface name, run one of:

```
ifconfig eth0 10.72.9.12
ifconfig eth1 10.72.9.12
ifconfig enp3s0 10.72.9.12
```

   If you're workstation has only one ethernet connection and the new firewall is plugged into a switch that connects to the workstation, set a second IP address on the primary ethernet interface. It will likely be this:

```
ifconfig eth0:0 10.72.9.12
```

2. On your Debian workstation, point your browser to the IP address you set on the LAN interface. For example, https://10.72.9.254/

3. Your browser will issue a warning about the SSL certificate.

```
Your connection is not private

Attackers might be trying to steal your information from 10.72.9.254
↪   (for example, passwords, messages, or credit cards).
↪   NET::ERR_CERT_AUTHORITY_INVALID
```

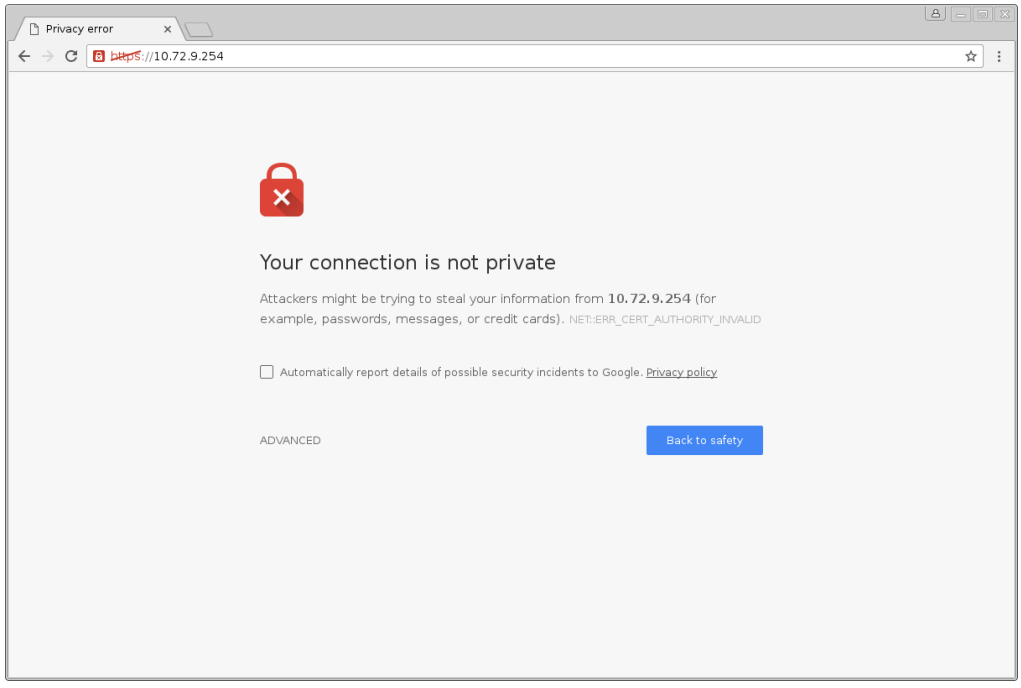

Figure 1.4: pfSense Cert Authority Invalid

4. In your browser hit Advanced, which will display this text:

```
This server could not prove that it is 10.72.9.254; its security
 ↪   certificate is not trusted by your computer's operating system.
 ↪   This may be caused by a misconfiguration or an attacker
 ↪   intercepting your connection.

Proceed to 10.72.9.254 (unsafe)
```

5. Click Proceed to go through with this operation. A new SSL cert will be set up on the firewall in later steps.

6. Log in to firewall (e.g. https://10.72.9.254). The initial username is admin and the password is pfsense.

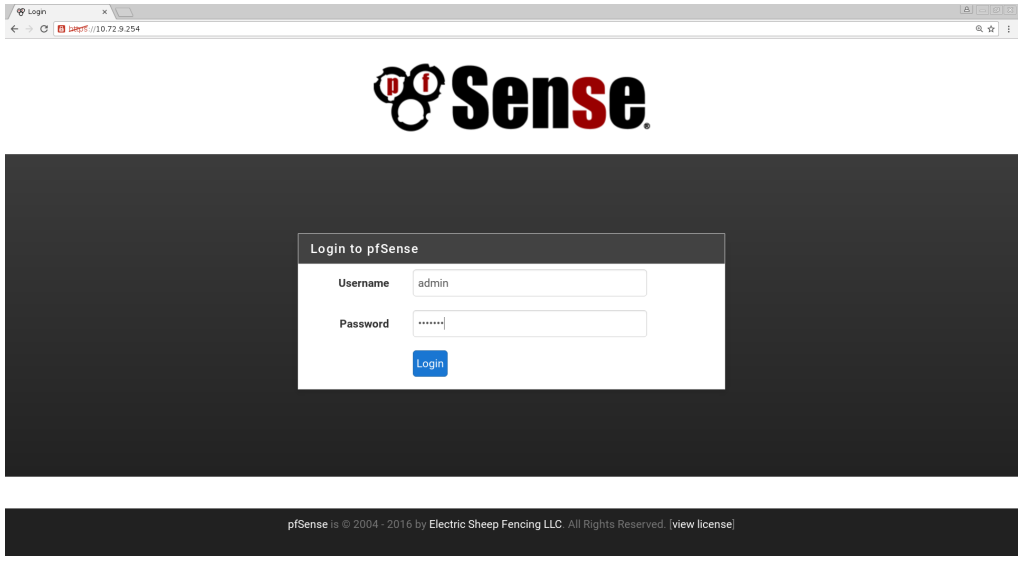

Figure 1.5: pfSense Login

7. Start Wizard, hit Next.

8. pfSense Gold, Next.

9. Hostname: set hostname and domain. In this example, fw729 and alephobjects.com. DNS servers can be blank for now.

10. Time Server Hostname, leave at default. Set timezone to America/Denver.

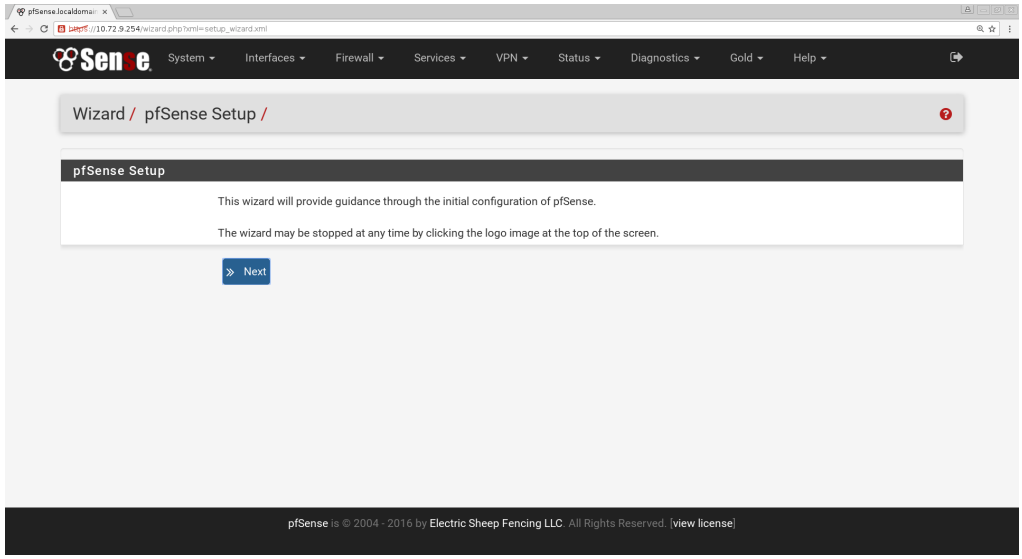

Figure 1.6: pfSense Wizard

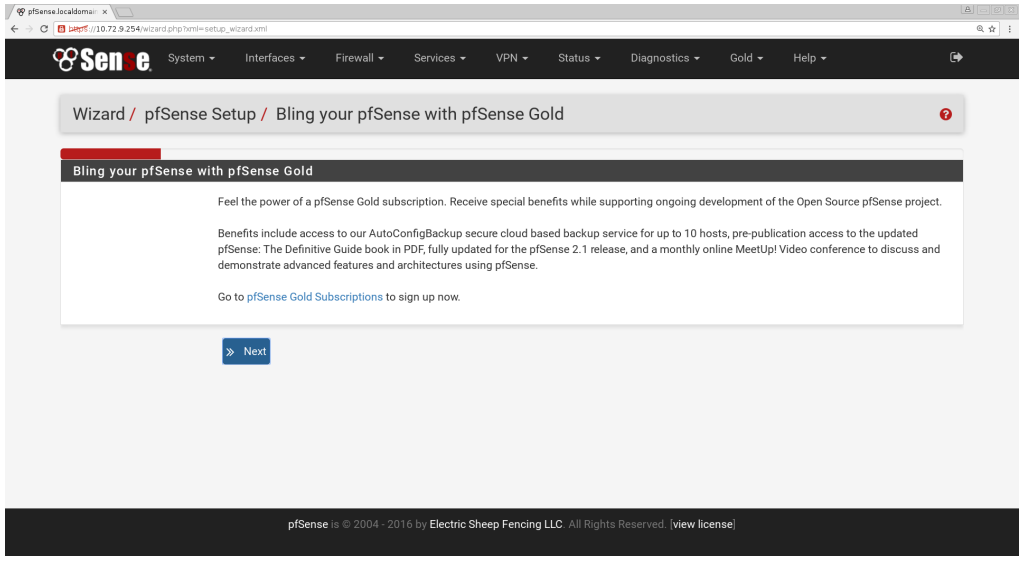

Figure 1.7: pfSense Gold

11. Configure WAN interface. Leave the WAN interface ethernet cable unplugged. In later steps, once we get the basic firewalling etc.

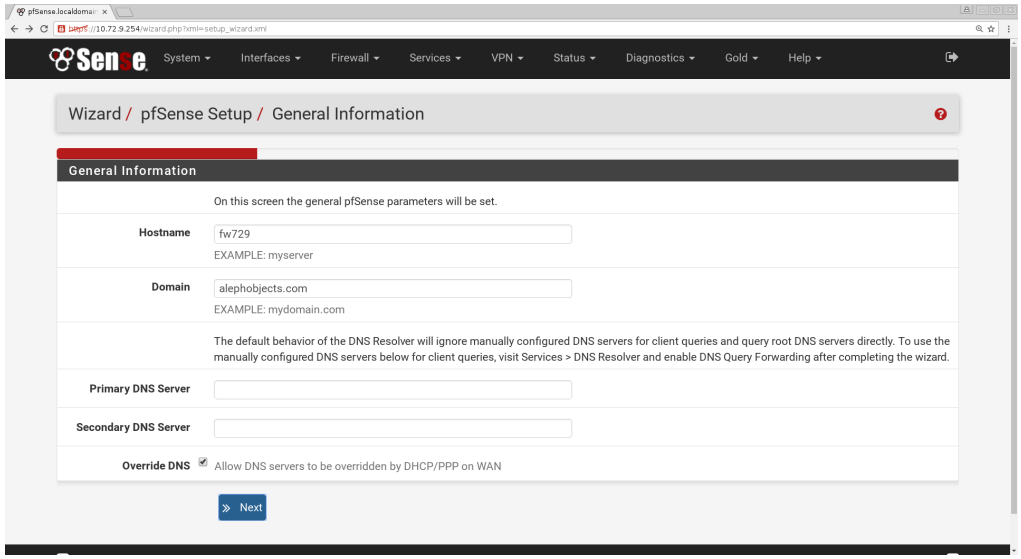

Figure 1.8: pfSense Wizard General Information

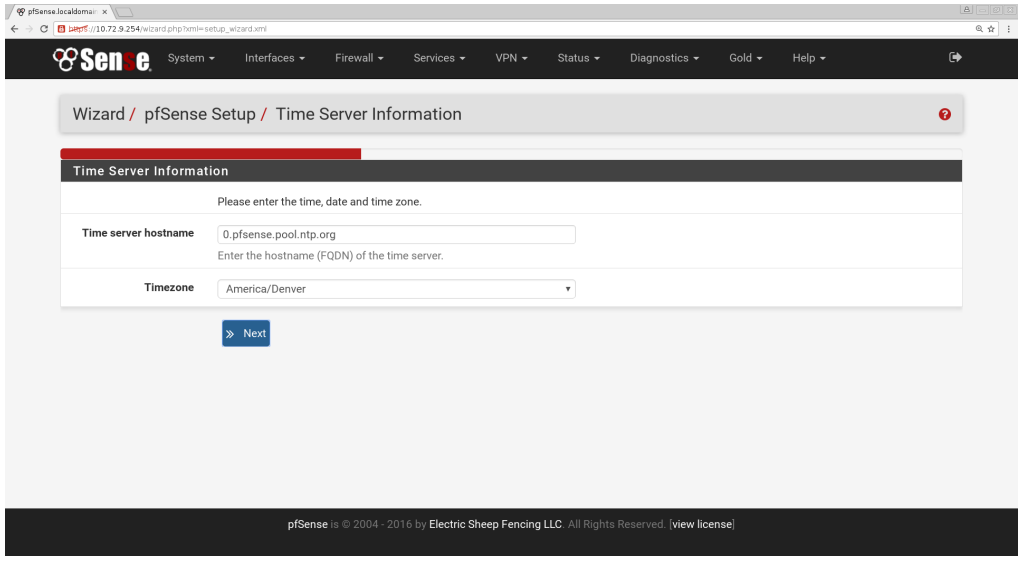

Figure 1.9: pfSense Wizard Timezone

running, we can plug in WAN and configure it. For now, take the WAN DHCP defaults.

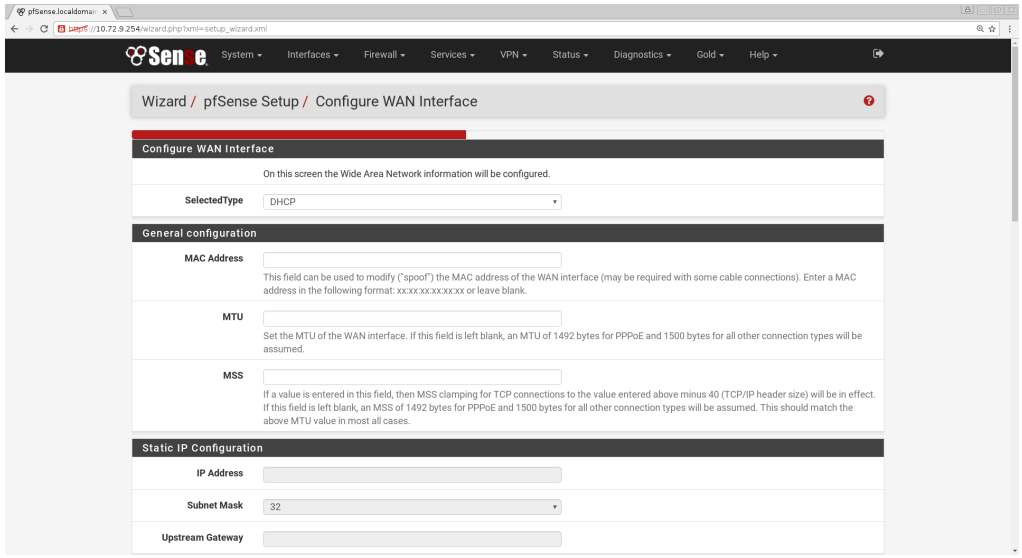

Figure 1.10: pfSense Wizard WAN Configuration

12. Configure LAN interface. Set the static IP and netmask, in this example 10.72.9.254 and 24.

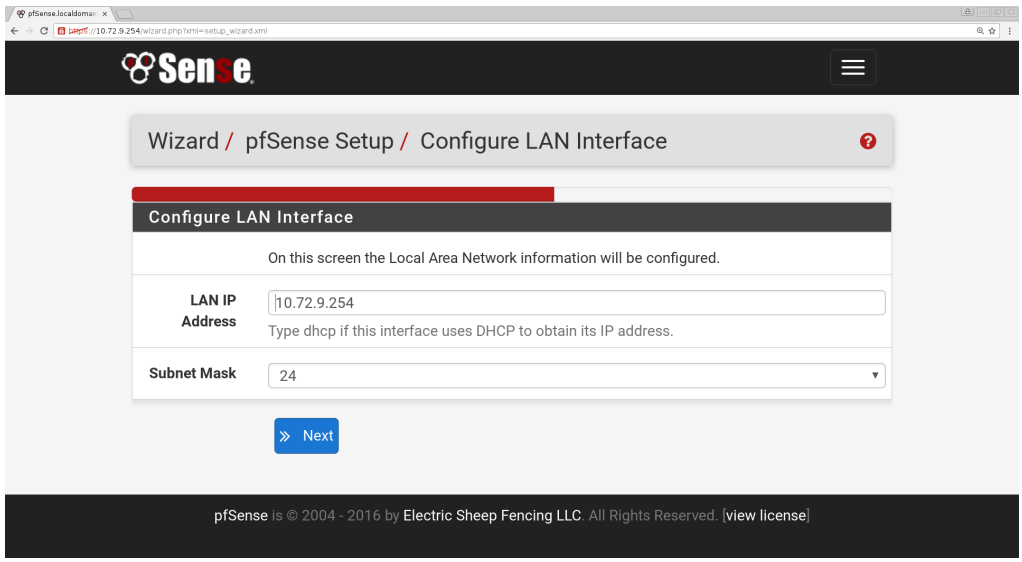

Figure 1.11: pfSense Wizard LAN Configuration

13. Set Admin WebGUI Password. Choose something unique and following good practices. Use a good password generator.

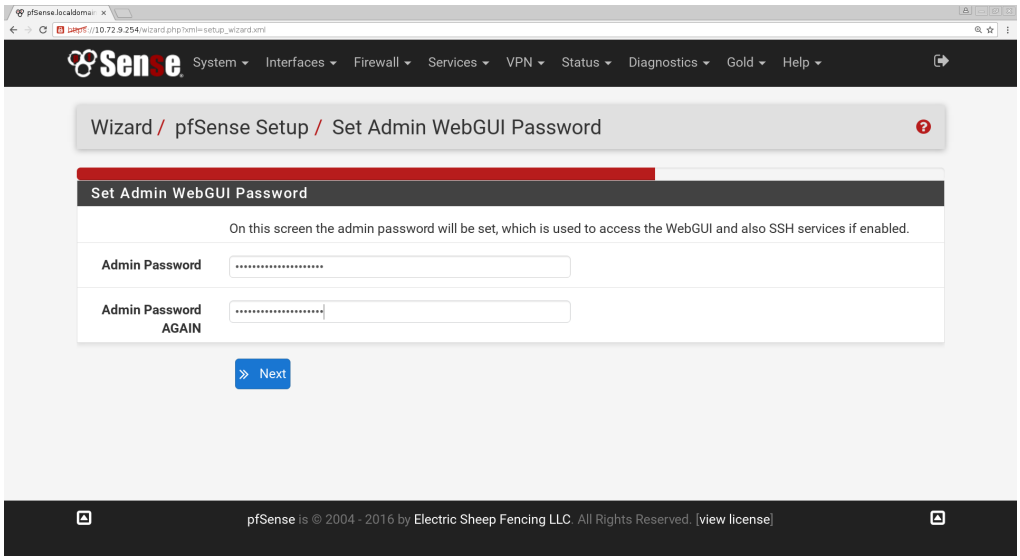

Figure 1.12: pfSense Wizard Admin Password

14. Hit Reload to use the new configuration.
15. Watch wizard reload. This should take less than a minute.
16. The wizard is now complete. Click `here` in `Click here to continue on to pfSense webConfigurator.`

1.2.4 Moar Configuration

Now that the basic setup of the firewall is done...there is more... Upon logging in the first time, you are greeted with a basic Dashboard. Menu items are across the top.

1. System –> User Manager. Click Add. Add Username, Password, Full name, Experation date leave blank. Move to add to Group membership “admins” (presuming this is an admin). Add ssh key, if you want to ssh in. Certificate, leave blank for now (can be used for OpenVPN/RADIUS).

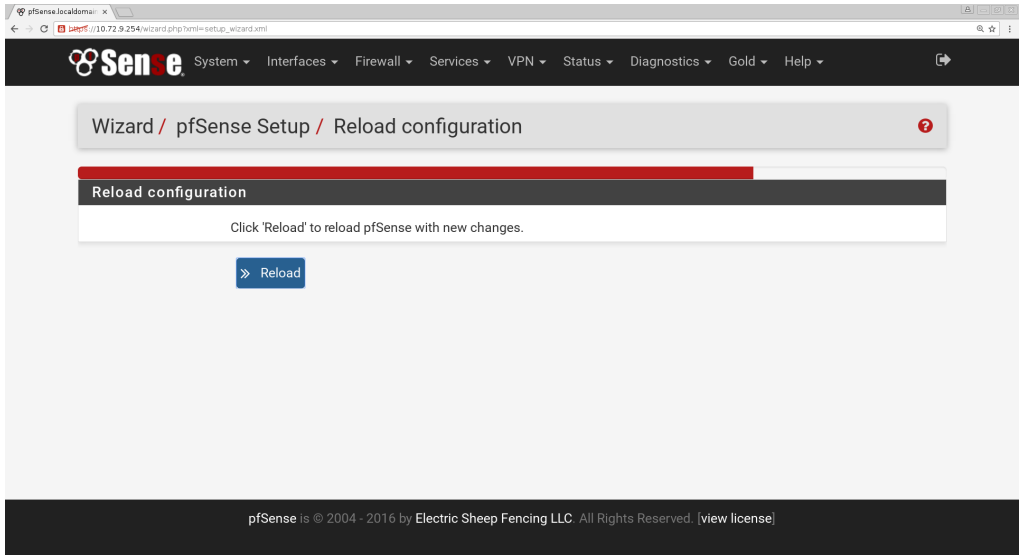

Figure 1.13: pfSense Wizard Reload Configuration

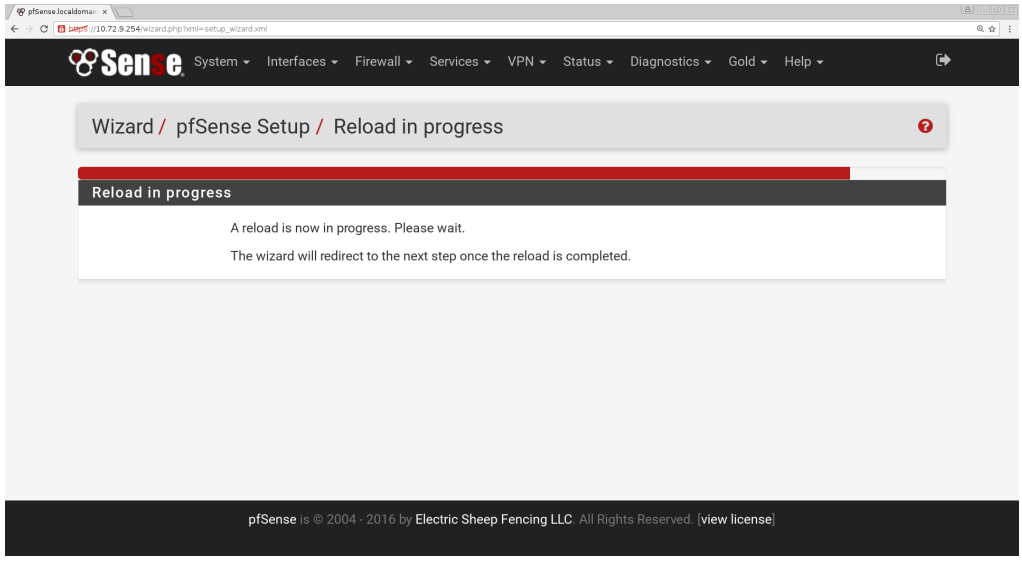

Figure 1.14: pfSense Wizard Reloading

2. Log out and log back in as newly created user.

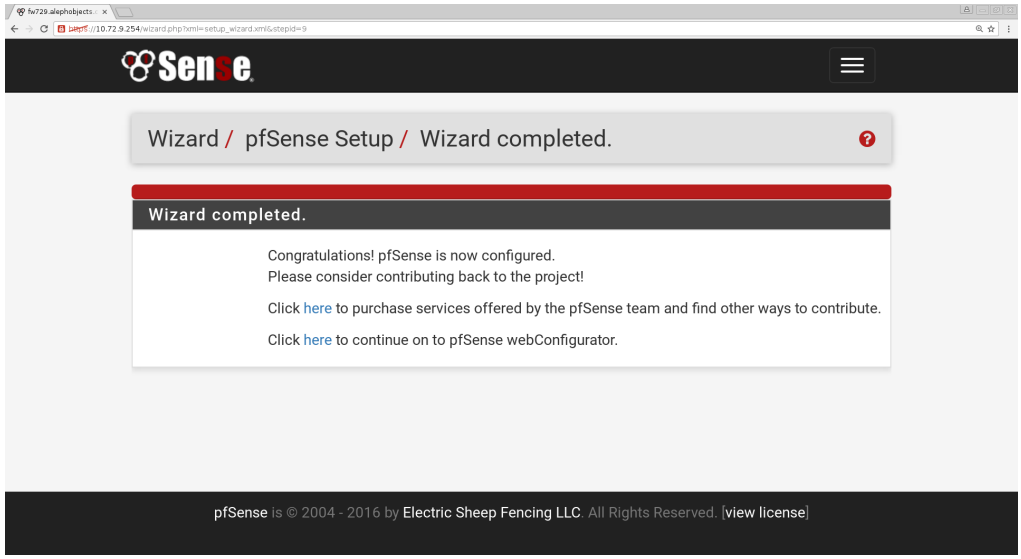

Figure 1.15: pfSense Wizard Reloading

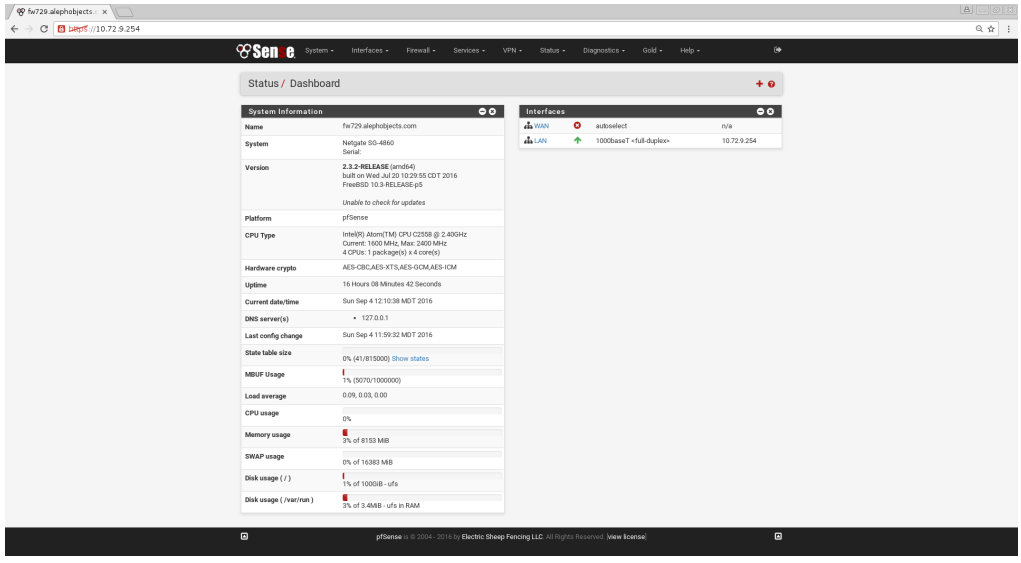

Figure 1.16: pfSense Initial Dashboard

3. Goto System –> Advanced. Under Admin Access. Set TCP port to randomish port between 1 and 65535. This will be the new pfSense

web interface port address. Max processes: 16 (2 is too low, not sure what is ideal). Check WebGUI redirect to disable port 80. Check enable Secure Shell Server. Disable password login. Pick randomish port for SSH. Check to password protect Console menu. Save.

4. At this point, you can optionally SSH into the firewall if a key was set up for the user.

5. Under System –> Advanced, Networking. Uncheck Allow IPv6, to disable IPv6 (yay!). Check boxes for: Hardware Checksum Offloading, Hardware TCP Segmentation Offloading, Hardware Large Receive Offloading. These need to be disabled because/if Suricata is used in Inline mode. If it isn't, these can be unchecked and if the hardware is good/can handle it, it will likely be faster. (Side note, enabling Hardware Checksum Offloading breaks networking in a KVM.) Save.

6. System –> Advanced, Miscellaneous. Cryptographic Hardware should be set to AES-NI for any hardware from pfSense. For other hardware, check dmesg. Thermal Sensors: Intel Core* CPU on-die thermal sensor. Hard disk standby time, 6 minutes (not sure this really has any effect). Host UUID, check Do NOT send HOST UUID with user agent. Save.

7. System –> Notifications. Check for Disable Growl Notifications and Disable SMTP. Save.

1.2.5 SSL Certificate Manager Setup

1. System –> Cert. Manager. Under Certificates, click Add. Method: Create a Certificate Signing Request. Descriptive Name, use the hostname of the firewall being setup. Key length 4096, Digest Algorithm sha512. Country Code US, etc. Common name, use hostname of firewall. Save.

2. System –> Cert. Manager, Under Certificates, the new cert added above, click Export Request mini-icon. Gandi: Standard SSL, single address, 3 year. Paste in the CSR exported from the mini-icon into Gandi. Select Apache/ModSSL for Software used in Gandi, and if it says the correct "Main domain (CN)", hit Submit in Gandi. Delete any .req file that was downloaded by browser. Gandi: Validation by

email (probably). It will take 10+ minutes to get verification back from Gandi (not instant).

3. System –> Cert. Manager, Under Certificates. When cert is ready and confirmed at Gandi, hit Get the Certificate. Hit the "Update CSR" pencil on the appropriate certificate line. Paste the Gandi cert into Final certificate data. Delete any downloaded copies.

4. System –> Cert. Manager. Under CAs, click Add. Method: Import an existing Certificate Authority. Descriptive Name: "GandiStandardSSLCA2". Get the cert from https://www.gandi.net/static/CAs/GandiStandardSSLCA2.pem and paste into Certificate data. Certificate Private Key, blank. Save. Note, this has to be done after the above Gandi certificate is added to the firewall.

5. System –> Cert. Manager, also import any of our own CAs and Certificate Revocations, if any.

1.2.6 General Setup

1. System –> General Setup. Check all looks good. Top Navigation: Fixed (Remains visible at top of page). Hostname in Menu: Hostname only. (DNS servers can be bound to particular interfaces here, if needed in multi-WAN). Save.

2. To use the newly set up certifcate. System –> Advanced, Admin Acess. Change SSL Certificate to the new one. Save. Now go to that new hostname with https and the correct port.

1.2.7 Initial Firewall Rules

1. Firewall –> Rules. LAN interface, click the pencil to edit the IPv6 line. Change Action to Reject. Change Source to any. Change Description to "Default Reject LAN IPv6". Save. Apply Changes.

2. Firewall –> Rules. Under LAN interface, click the Copy mini-icon to copy the IPv6 line. Change Action to Block. Interface to WAN. Change Description to "Default Block WAN IPv6". Save. Apply Changes.

1.2.8 Initial DNS Resolver Setup

1. Services –> DNS Resolver. Enable (default). Network Interfaces: just select LAN and localhost. Outgoing Network Interfaces: WAN, LAN, localhost. Add checks for DHCP Registration, Static DHCP. Save. Apply Changes.

2. Services –> DNS Resolver, Advanced Settings. Add checks for: Prefetch Support, Prefetch DNS Key Support. Increase Message Cache Size to 50 MB or so (?). Save. Apply Changes.

3. Services –> Dynamic DNS. Setup, if needed.

1.2.9 Initial Logging Setup

Setup logging to the local firewall. Remote logging will be set up.

1. Status –> System Logs, Settings. Add checks to Forward/Reverse Display. GUI Log Entries, increase to 200. Where to show rule descriptions "Display as second row". This is where remote logging will be set up...

2. Status –> Dashboard. Click the Plus + in the upper right corner. Add the available widgets: Gateways, Thermal Sensors, Traffic Graphs, S.M.A.R.T. Status, Firewall Logs, Interface Statistics, OpenVPN, Services Status, NTP Status.

1.2.10 Backup

Make first backup.

1. Diagnostics –> Backup & Restore. Backup.

2. Diagnostics –> Reboot and make sure everything comes up clean.

1.2.11 Internet Connection

Make initial connection to the Internet with the new pfSense firewall.

At this point, this presumes the WAN interface isn't up and routing actual Internet traffic. It is better to get the router as configured as

possible before actually using the WAN interface. Assuming the firewall is on the LAN and being configured, it can use the gateway that is on its LAN interface. When configuration is finalized and the router is deployed, the WAN interface will carry Internet traffic. To to this, add a route by: Interfaces –> LAN. Under IPv4 Upstream gateway, click Add a new gateway. Add the LAN gateway info, and check is as Default gateway (3000). Save. Apply Changes..

1. System –> Routing. Click to edit the mini pencil icon on the Gateway line listed as Default. Monitor IP: something appropriate upstream, can use 8.8.8.8. Note: on high latency connections such as satellite, hit Display Advanced and increase Latency thresholds (750, 2500), Packet Loss thresholds (15, 25), Probe Interval (1000), Loss Interval (3000). Save. Apply Changes.

1.2.12 Update & Install Packages

1. System –> Update, System Update. Check that the Status is "Up to date." If it needs updating, update.

2. System –> Package Manager, Installed Packages. The first time here, you need to click on Available Packages (presumably to download latest package header info). Then go back to Installed Packages. If there are any Installed Packages that have a Newer version available, click the mini icon to update the package. Confirm.

3. System –> Package Manager, Available Packages. Install: Cron, ntopng, openvpn-client-export, pfBlockerNG, RRD_Summary, Status_Traffic_Totals, sudo, suricata.

4. System –> sudo. Add user, optionally.

1.2.13 OpenVPN

OpenVPN is run by a collection of pfSense firewalls.

1. OpenVPN setup.

2. System –> Cert. Manager. Set up internal certificate authority.

3. System –> Cert. Manager. Create internal server certificate.

4. SSH into firewall. pfSense ships with pre-generated DH keys, due to "heavy computation". This can take an hour for 4096.

```
/usr/bin/openssl dhparam 1024 >
↪  /etc/dh-parameters.1024
/usr/bin/openssl dhparam 2048 >
↪  /etc/dh-parameters.2048
/usr/bin/openssl dhparam 4096 >
↪  /etc/dh-parameters.4096
```

5. VPN –> OpenVPN. Set up VPN server. Server Mode: Remote Access (SSL/TLS + User Auth). Backend for Authentication: Local Database (will be FreeRADIUS at some point). Protocol: UDP. Local Port: something randomish. Peer Certificate Authority: use the interal CA created earlier. Server Certificate: Use the server certificate created earlier. DH Parameter length (bits): 4096. Encryption Algorithm: AES-256-CBC (256-bit), this has hardware crypto support on pfSense routers. Auth digest algorithm: SHA512 (512-bit). Hardware Crypto: BSD Cryptodev engine- RSA, DSA, DH, AES-128-CBC, AES-192-CBC, AES-256-CBC. Certificate Depth: One. Strict User-CN Matching: check Enforce Match once it is confirmed working. IPv4 Tunnel Network: Set the new VPN network. IPv6 Tunnel Network: leave blank. Redirect Gateway: unchecked. IPv4 Local network(s): set the local LAN network. IPv6 Local network(s): leave blank. Compression: Enabled with Adaptive Compression. Inter-client communication: Checked. Disable IPv6: Checked. Dynamic IP: Unchecked, at least for now. Topology: subnet. DNS Default Domain: Checked, and set domain. DNS Server enable: Checked. DNS Server 1: enter servers. Save.

6. System –> User Manager. Add user for VPN. Certificate: Check to create user certificate. Descriptive name: username.domainname. Certificate Authority: Select internal CA created above. Key length: 4096. Lifetime: 1095.

7. VPN –> OpenVPN, Client Export. Remote Access Server: Select the VPN server created earlier. Verify Server CN: automatic.

Block Outside DNS: Checked. At the bottom, export as Standard Configurations, Archive to use with another pfSense server. To use with OpenVPN in F-Droid (Android), use Inline Configurations (Android).

1.2.14 Turn off Internet via LAN

1. Interfaces –> LAN. When you're done using the LAN as any sort of gateway. Change IPv4 Upstream gateway to None. Save. Apply Changes.

1.2.15 More Backup

Make another backup.

1. Diagnostics –> Backup & Restore. Backup.
2. Diagnostics –> Reboot and make sure everything comes up clean.

1.3 NAT

Network Address Translation.

- VoIP using SIP is often a problem behind a NAT.
- Enable Keepalives in Grandstream phones to connect to the Asterisk server.
- Disable ALG (Application Level Gateway) in any consumer/home routers.

1.4 Traffic Shaping

- Prioritize admin ssh to firewalls/servers (in case of DoS, etc.)
- Prioritize VoIP
- De-prioritize SMTP, etc...

1.5 pfBlockerNG

- IP blocklists for botnets, etc.

1.6 Suricata

Suricata is being used as an Intrusion Detection System. It is preferred over Snort as Suricata is multithreaded and Snort isn't.

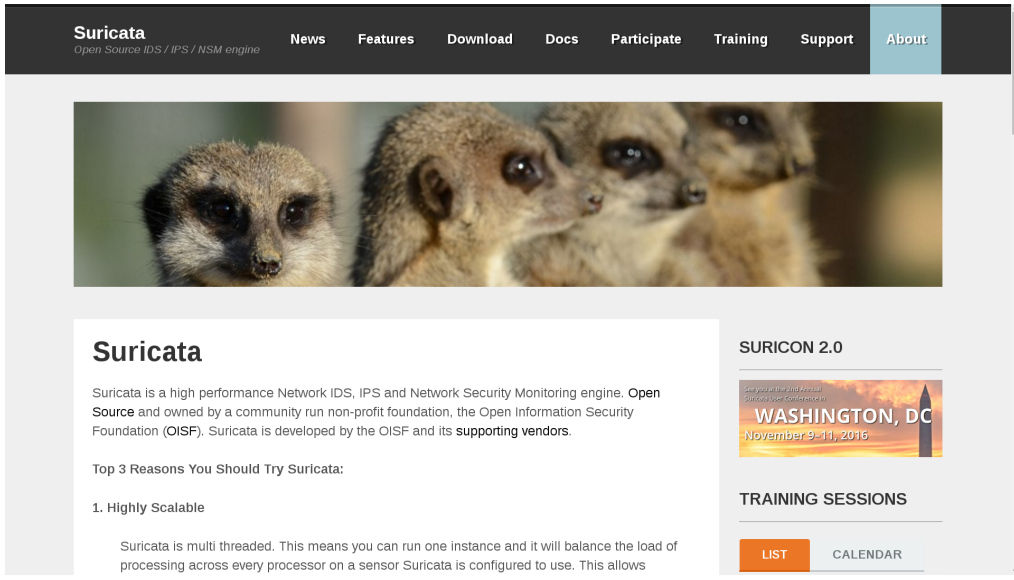

Figure 1.17: Suricata Website

- barnyard2
- Snort Blacklists
- Emerging Threats Blacklists
- GeoIP
- Alerts, Blocks, Suppress
- SID

1.7 DHCP

For DHCP services, pfSense uses Dnsmasq, which is also used for DNS forwarding.

1. Services –> DHCP Server. Network Booting, click Display Advanced. Check box for Enables Network Booting. Set Default BIOS file name to jessie_crypto/pxelinux.0 or jessie/pxelinux.0. Set Next Server to IP address of tftp server. Save.
2. Services –> DHCP Server. Go to the bottom and hit Add. Add the MAC address, Client Identifier (hostname), IP Address, Hostname, Netboot Filename (we probably don't need it in the general config), and TFTP Server.

- Disable IPv6.
- tftp netboot installs.
- Static mappings.

1.8 NTP

1.9 OpenVPN

Virtual Private Networks.

OpenVPN — "OpenVPN is a full-featured open source SSL VPN solution that accommodates a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls."

- Network design (e.g. many point to point, one central server, etc.).
- Main OpenVPN server.
- Other internal servers.
- External servers private connections.
- Laptops.

Figure 1.18: OpenVPN Website

- Mobiles.
- SSL certificates.
- AES-256-CBC is hardware accelerated on pfSense routers.
- SHA512 Auth digest algorithm
- Hardware Crypto: BSD cryptodev engine

pfSense ships with pre-generated DH keys, due to "heavy computation". This can take an hour for 4096.

```
/usr/bin/openssl dhparam 1024 > /etc/dh-parameters.1024
/usr/bin/openssl dhparam 2048 > /etc/dh-parameters.2048
/usr/bin/openssl dhparam 4096 > /etc/dh-parameters.4096
```

1.10 Captive Portal

The Captive Portal for Aleph Mountain building wifi services.

1.11 SSL Certificates

pfSense makes it very easy to generate Certificate Signing Requests (CSRs), which can be send to Gandi.net to get issued a "properly" signed SSL certificate.

1.12 ssh

OpenSSH from OpenBSD is used. The BSD shell is a bit different from GNU.

1.13 DNS

DNS forwarding is provided by Dnsmasq.

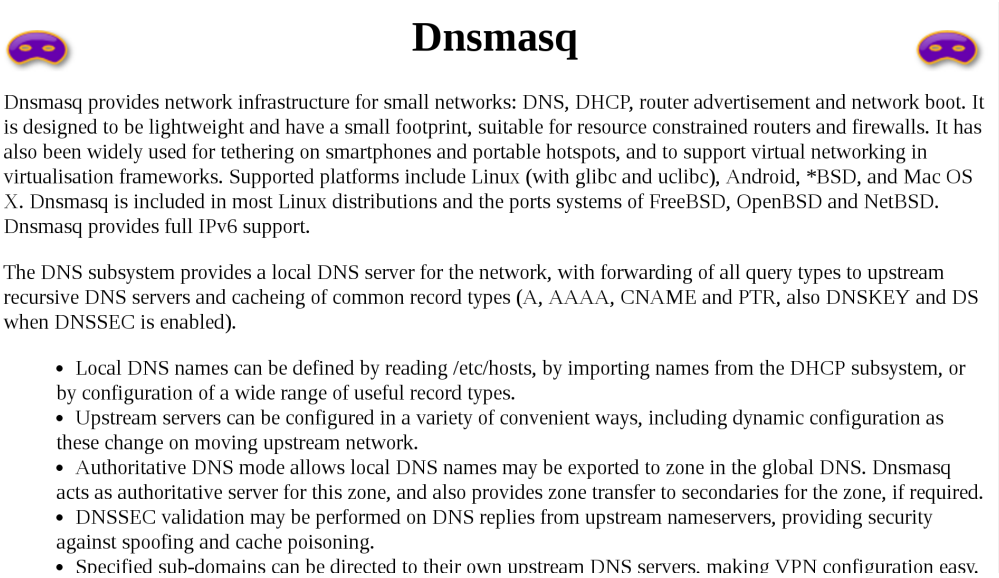

Figure 1.19: Dnsmasq Website

1.14 Routing

- No BGP, OSPF, etc.

- Static backbone routes.
- WAN failover

1.15 Interfaces

- Gigabit ethernet.
- SFP+.
- Hardware offloading (e.g. checksums).

1.16 CARP and Synchronization

CARP can be used to have transparent failover to another firewall, if one firewall on the network should drop.

Synchronization between CARP firewalls allows easy configuration updates. For instance, if a configuration change is made to the DHCP server, it can "instantly" push to the backup firewall.

1.17 Reporting

- Dashboard.
- Darkstat.
- ntopng ("Network Top Next Generation" ?).
- S.M.A.R.T.
- System Temperatures.
- MRTG
- RRD

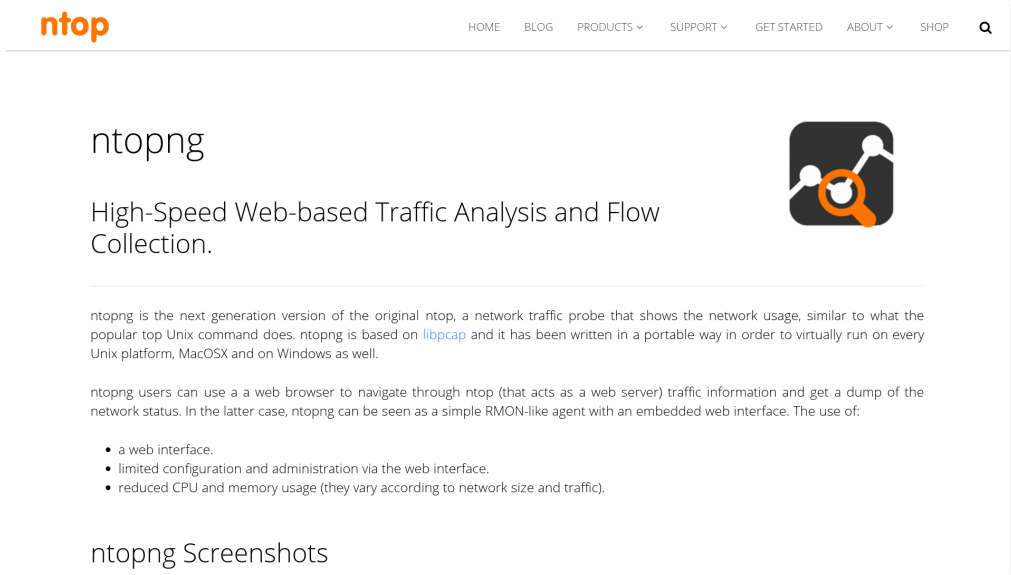

Figure 1.20: ntopng Website

iptables

Stop.

2.1 Overview

Aleph Objects has recently deployed pfSense firewalls, replacing OpenBSD. Most servers and workstations run GNU/Linux, which uses iptables.

2.2 iptables

iptables is part of the Netfilter project and has been included by default in the Linux kernel for many years.

Figure 2.1: Netfilter Website

Hardware

Purchase Order

3.1 Overview

Hardware.

- (8) 1 gig ethernet ports Connects to (1) 100M ethernet upstream fiber optic Connects to (1) 100M ethernet upstream wifi Various LAN
- (Hot swap?) Dual Power Supplies
- (How swap?) RAID (Linux md), with SSD storage.
- 2.5” drive bays
- Total 8GHz CPU
- 8-16 gigs RAM ? Depends on OS.
- Two servers total, for standby/failover

Switches

Here.

4.1 Overview

There are free software solutions for network switches, allegedly. Lets see.

Currently, the network is using 1 gig-e basically everywhere, except phones which are 100M (and so is anything plugged into them). The Internet backbone connection is 500M fiber, plus unlicensed wifi. An additional 1 gig backbone connection to another provider is being evaluated.

We need a few hundred gig-e ports, with 10 gig uplinks using SFP+ fiber. Around six 48-port switches, plus more if we add co-location.

4.2 Free Software for Network Switches

4.2.1 ONIE

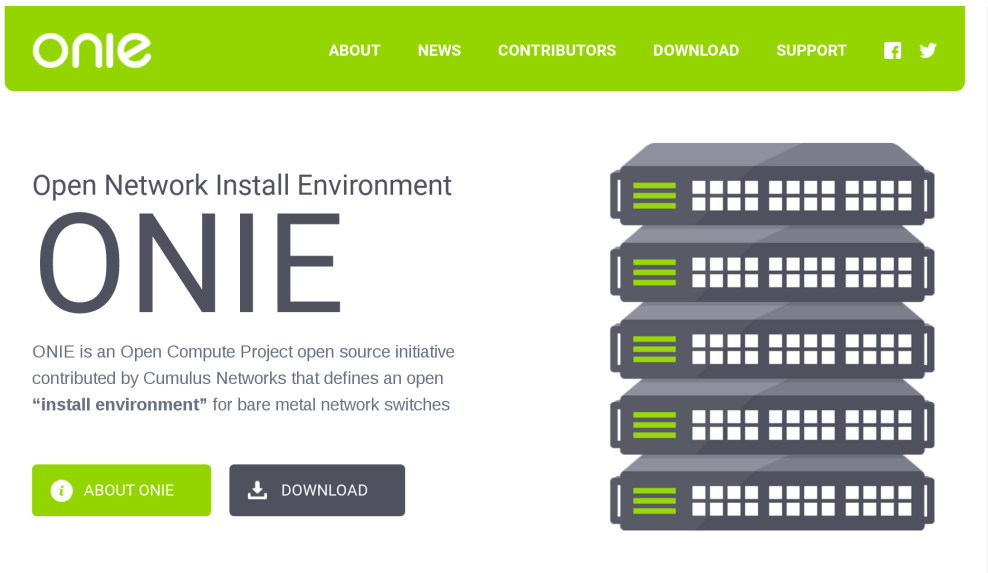

Figure 4.1: ONIE Website

- Website:
  http://onie.org
- Source code:
  https://github.com/opencomputeproject/onie

- Wiki:
  https://github.com/opencomputeproject/onie/wiki
- License: GPLv2
- Hardware status:
  http://www.opencompute.org/wiki/Networking/ONIE/HW_Status
- Operating System Support:
  http://www.opencompute.org/wiki/Networking/ONIE/NOS_Status

"The Open Network Install Environment (ONIE) is an Open Compute Project open source initiative driven by a community to define an open "install environment" for bare metal network switches, such as existing ODM switches and the upcoming OCP Network Switch design. ONIE enables a bare metal network switch ecosystem where end users have a choice among different network operating systems.... ONIE was contributed to the Open Compute Project.... ONIE is an open source "install environment", that acts as an enhanced boot loader utilizing facilities in a Linux/BusyBox environment. This small Linux operating system allows end-users and channel partners to install the target network OS as part of data center provisioning, in the fashion that servers are provisioned."

4.2.2 Open Network Linux

- Website:
  https://opennetlinux.org/

Distro for bare metal switches.
This is probably what we'll use. We'll see.
"Open Network Linux is a Linux distribution for "bare metal" switches, that is, network forwarding devices built from commodity components. ONL uses ONIE to install onto on-board flash memory. Open Network Linux is a part of the Open Compute Project and is a component in a growing collection of open source and commercial projects."
Supports these switch fabric APIs:

- OF-DPA

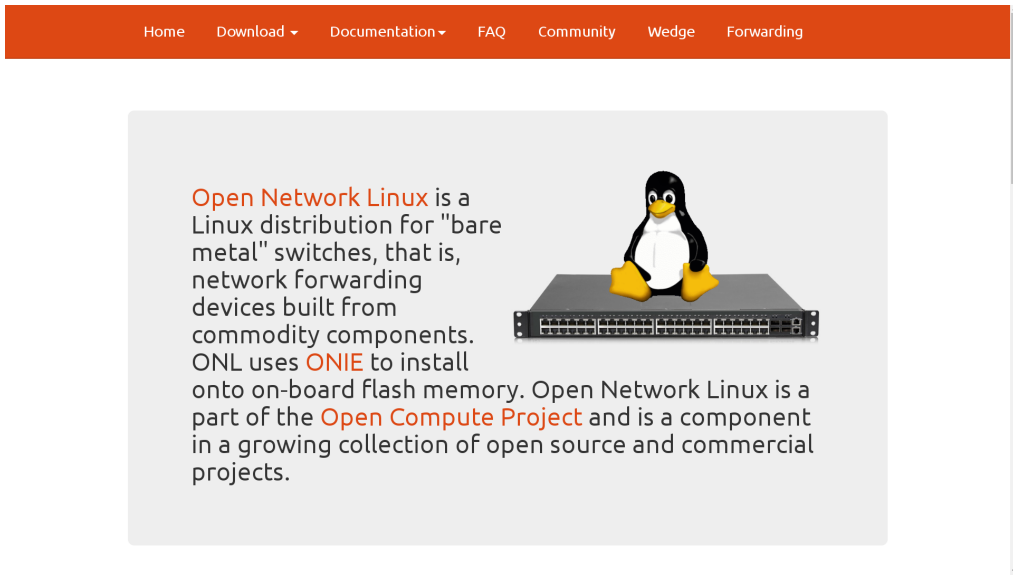

Figure 4.2: Open Network Linux Website

- OpenNSL — May be non-free Broadcom.
- SAI

Forwarding Agents:

- Quagga — "BGP4, BGP4+, OSPFv2, OSPFv3, IS-IS, RIPv1, RIPv2, and RIPng". In Debian.
- BIRD — "Internet routing daemon with full support for all the major routing protocols." In Debian.
- Facebook FBOSS — Open Source for Facebook scale.
- Azure SONiC — "SONiC is an open source project for network routers and switches"

4.2.3 Snaproute

- aka OpenSnaproute, FlexSwitch.

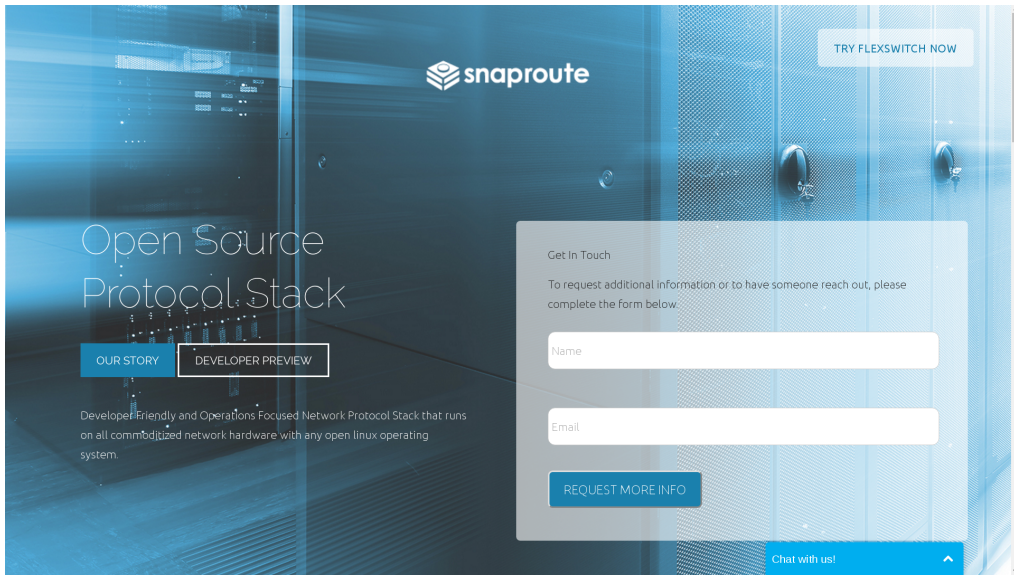

Figure 4.3: Snaproute Website

- Website:
  http://www.snaproute.com/
- Documentation:
  https://opensnaproute.github.io/docs/
- Written in Go programming language.

"Open source network stack for enterprise... Developer Friendly and Operations Focused Network Protocol Stack that runs on all commoditized network hardware with any open linux operating system."

4.2.4 OpenSwitch

- Website:
  http://www.openswitch.net/
- Linux Foundation project. Other big names.
- Hardware Compatibility (spoiler: Broadcom):
  http://www.openswitch.net/documents/user/hardware-compatibility

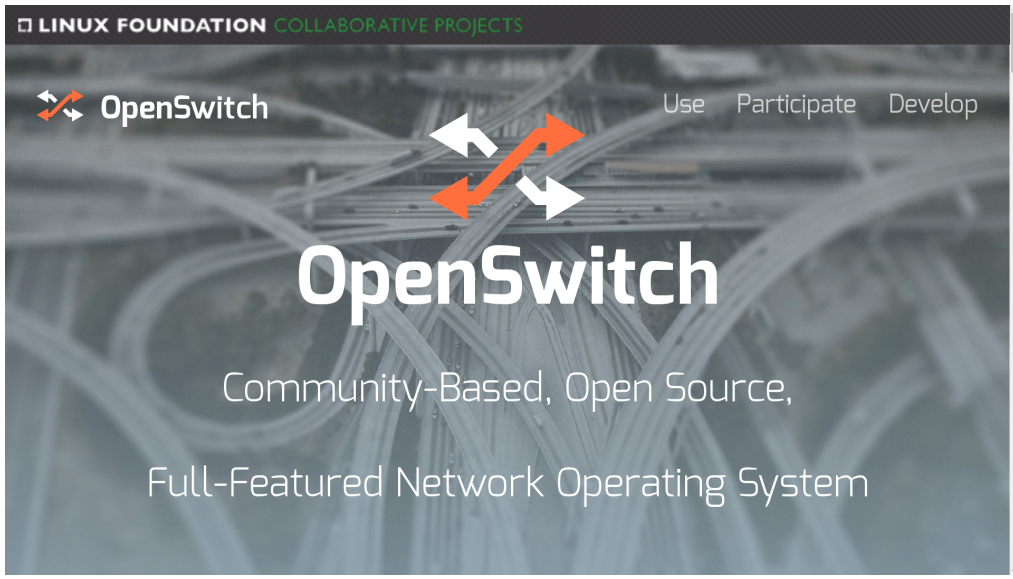

Figure 4.4: OpenSwitch Website

"Community-Based, Open Source, Full-Featured Network Operating System."

The hardware compatibilty list has Broadcom based systems from HPE Altoline and Edge-Core. All 10Gig+, high-end gear.

4.2.5 FBOSS

- Website:
  https://github.com/facebook/fboss
- Source code:
  https://github.com/facebook/fboss
- License: "BSD"

"Facebook Open Switching System (FBOSS). FBOSS is Facebook's software stack for controlling and managing network switches."

I am guessing this is going to be way overkill. Nom.

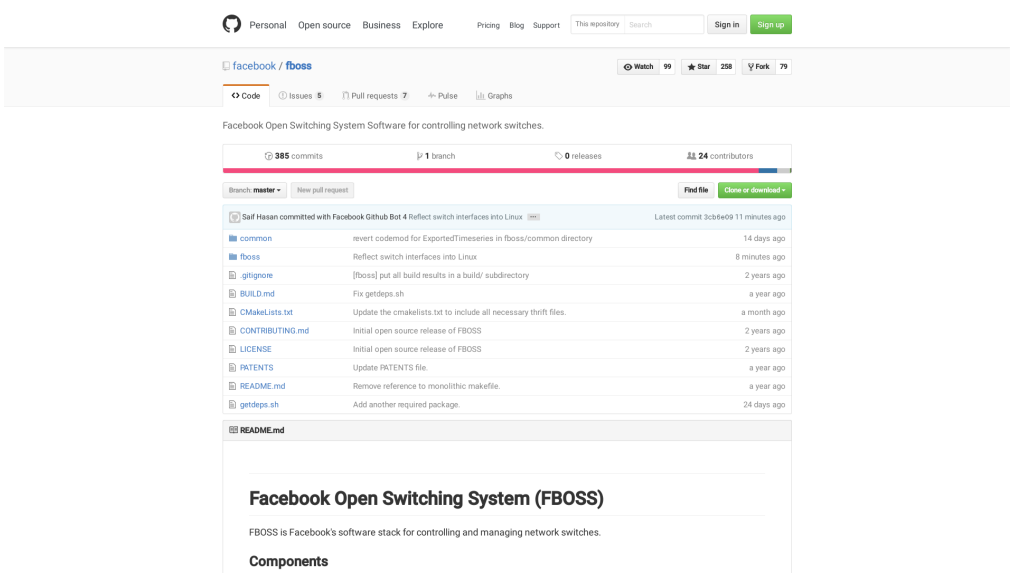

Figure 4.5: FBOSS Website

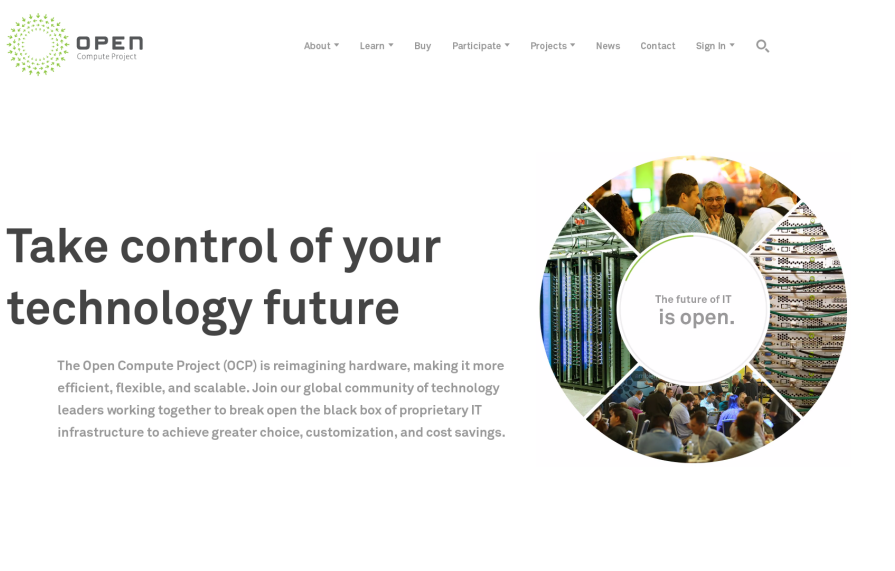

Figure 4.6: OpenCompute Website

4.2.6 Open Compute Project

- http://www.opencompute.org/
- http://github.com/opencomputeproject

"The Open Compute Project (OCP) is a collaborative community focused on redesigning hardware technology to efficiently support the growing demands on compute infrastructure."

Project so massive data centers can be more "open" and interoperate better between vendors, by using free software. Started by Facebook, supported by Google and others that run huge datacenters.

Although it is supposed to be an "Open Source" project, it includes non-free parts.

4.2.7 OpenDataPlane

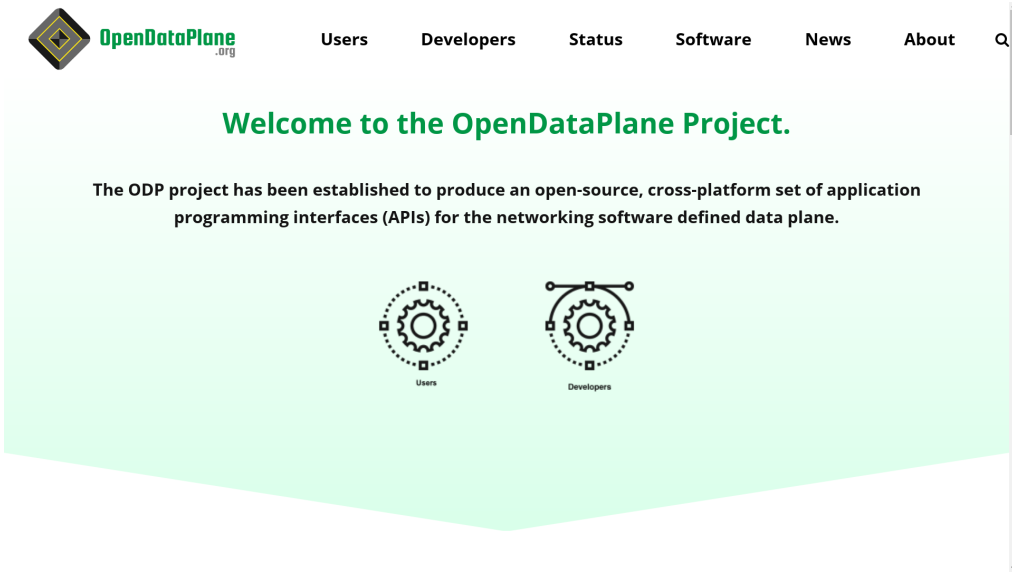

Figure 4.7: OpenDataPlane Website

- Website:
  http://opendataplane.org/

- Debian Apt Repository:
  http://deb.opendataplane.org/

"The ODP project has been established to produce an open-source, cross-platform set of application programming interfaces (APIs) for the networking software defined data plane."

These can run on top of ODP:

- OpenFastPath
  http://www.openfastpath.org/
- Open vSwitch
  http://openvswitch.org/

4.2.8 OpenFastPath

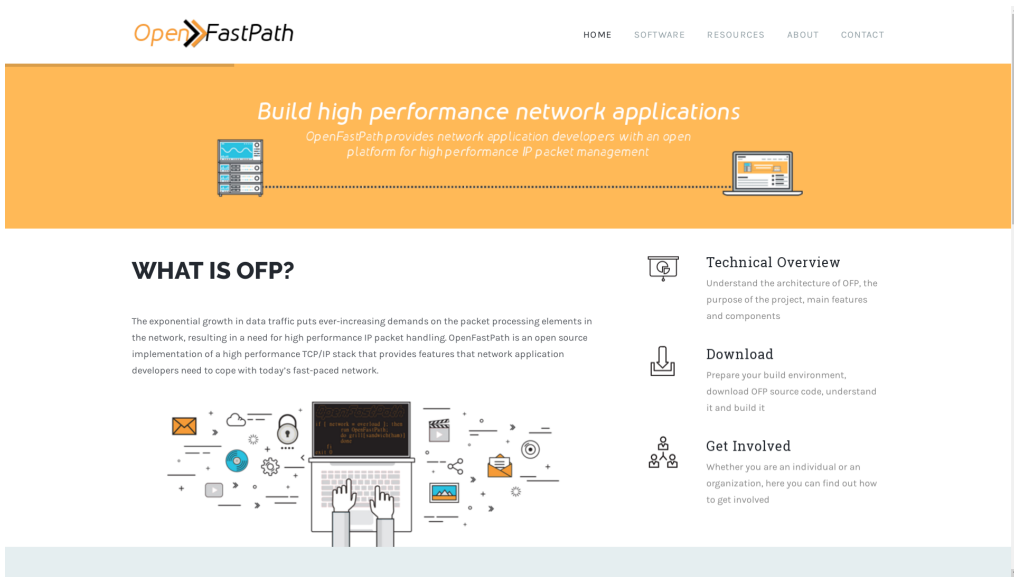

Figure 4.8: OpenFastPath Website

- Website:
  http://www.openfastpath.org/

"OpenFastPath is an open source implementation of a high performance TCP/IP stack that provides features that network application developers need to cope with today's fast-paced network."

4.2.9 Open vSwitch

Figure 4.9: Open vSwitch Website

- Website: http://openvswitch.org/
- Linux Foundation Project.
- In Debian.

"Open vSwitch is a production quality, multilayer virtual switch licensed under the open source Apache 2.0 license. It is designed to enable massive network automation through programmatic extension, while still supporting standard management interfaces and protocols (e.g. NetFlow, sFlow, IPFIX, RSPAN, CLI, LACP, 802.1ag)."

4.2.10 Big Switch

Figure 4.10: Big Switch Website, no

- Website:
  http://www.bigswitch.com/community-edition

Looks like baitware. Community version is more of a lame demo. Almost certainly no.

4.2.11 Uncategorized Software

- SAI — Switch Abstraction Interface.
- switchdev

SAI And Switchdev "SAI and switchdev are hardware abstraction models for switching silicon (ASICs). They are the open source frameworks that allow ASICs to be represented in software. This means you can use a Broadcom ASIC the same way as one from Mellanox or Cavium XPliant."

Microsoft's Azure Cloud Switch (ACS) is "Debian Jessie + SAI + everything else needed to power Azure (applications like Quagga, and the

switch state service based on Redis).” So their high end switching gear is based on free software, including Quagga and Redis...

4.3 Hardware

Hardware, on which to place free software.

4.3.1 Edge-Core

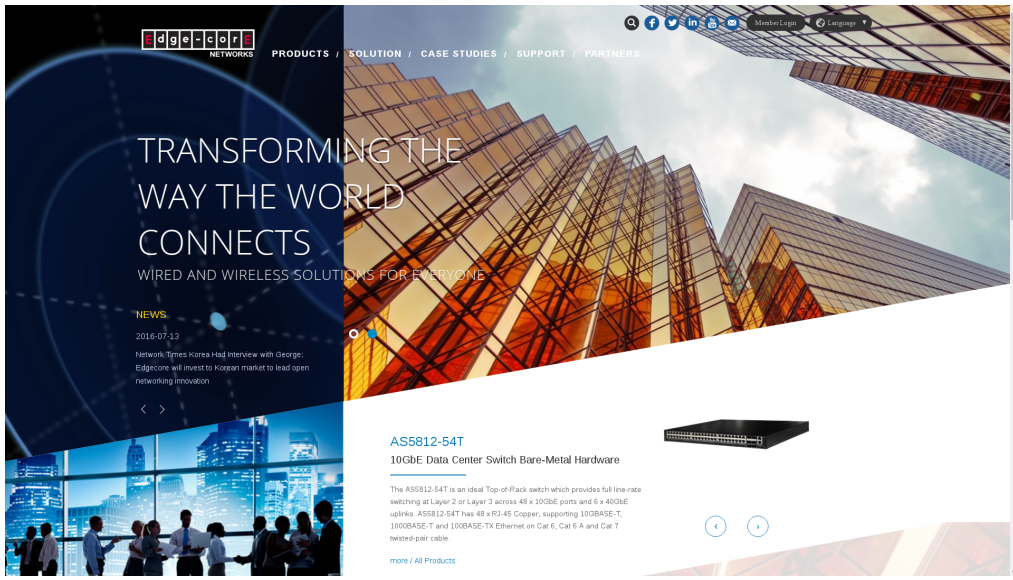

Figure 4.11: Edge-core Website

- Edge-Core — Owned by Accton
  http://www.edge-core.com/
- All Broadcom?

4.3.2 Dell

- Website:
  http://dell.com/

Dell makes some bare metal switches that are ONIE compatible.

4.3.3 Netberg

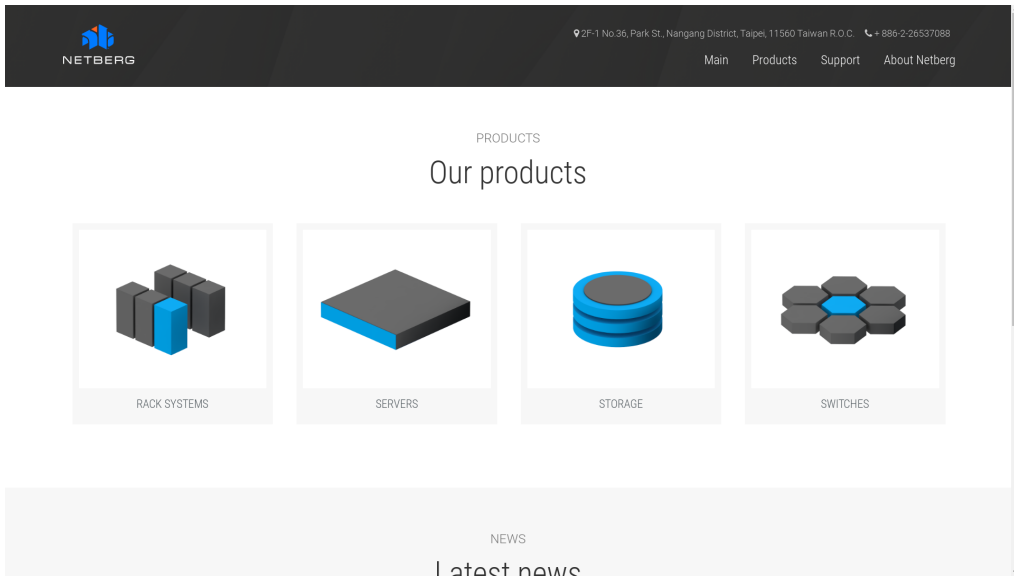

Figure 4.12: Netberg Website

- Website:
  http://netbergtw.com/

Netberg may be the manufacturer of some pfSense branded hardware. Appears to be...Broadcom based...

4.3.4 Quanta

- Website:
  http://www.qct.io/
- Sells "Bare Metal Switches (BMS)"

Uses...Broadcom.

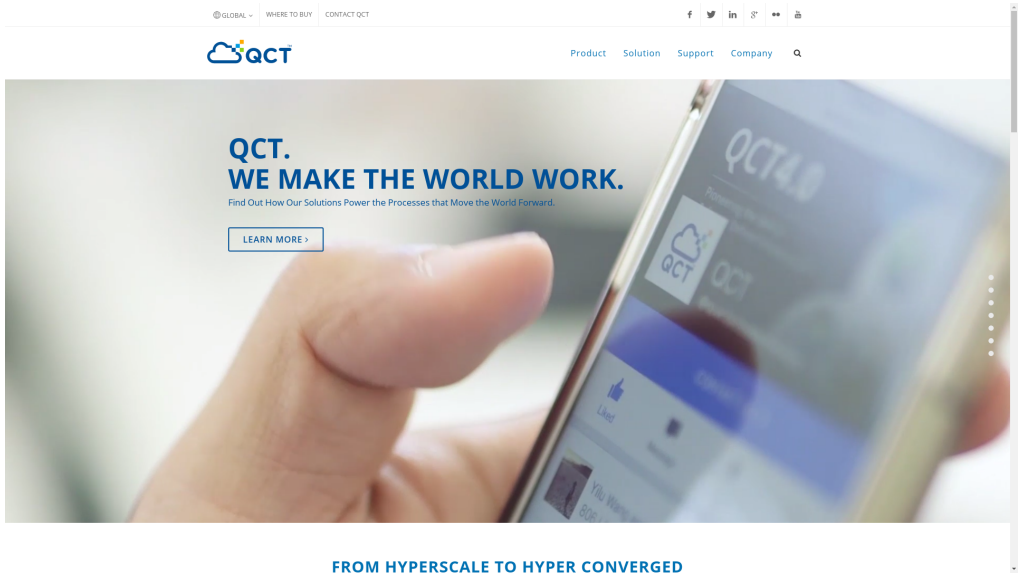

Figure 4.13: Quanta Website

4.3.5 Mellanox

Figure 4.14: Mellanox Website

- Website:
  http://www.mellanox.com/

High-end HPC gear, including switches and network cards.

4.4 Suppliers

4.4.1 White Box

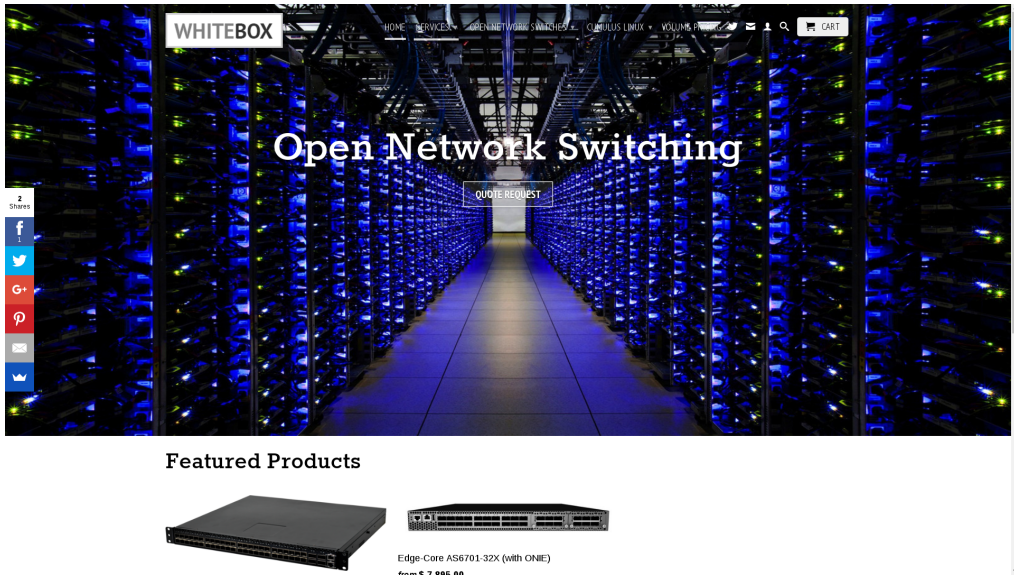

Figure 4.15: Whitebox Website

- Website:
  http://whiteboxswitch.com/
- Reseller of open switches.

1 Gig-e switches available:

- Edge-Core AS4600-54T
- Quanta T1048-LB9

10 Gig-e switches available:

- Edge-Core AS5610-52X (with ONIE)
- QuantaMesh BMS T3048-LY2R (with ONIE)

40 Gig-e switches available:

- Edge-Core AS6701-32X (with ONIE)
- QuantaMesh BMS T5032-LY6 (with ONIE)

These likely all.have.broadcom.

4.4.2 Bare Metal Switches

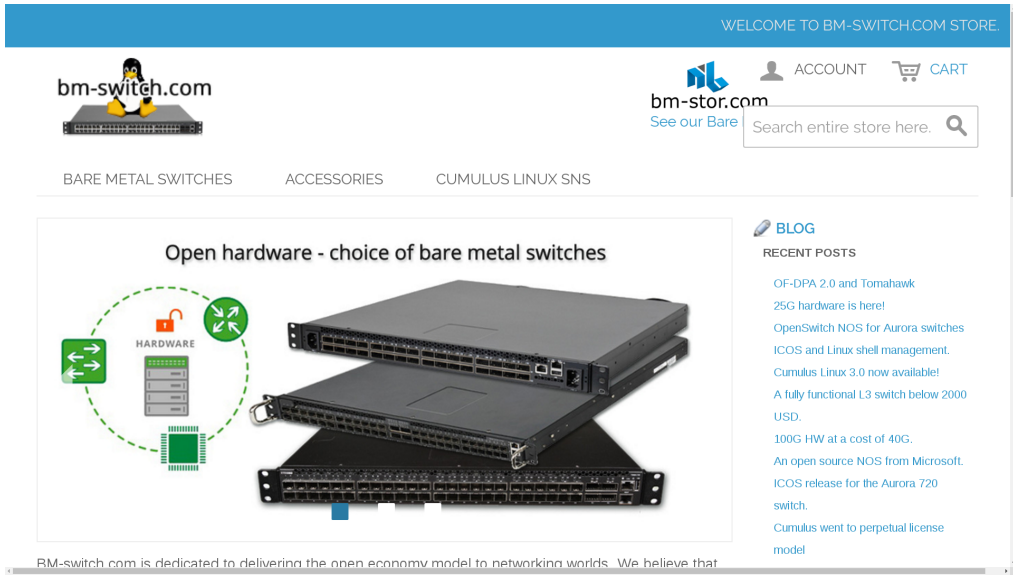

Figure 4.16: Bare Metal Switches Website

- Website:
  https://bm-switch.com/
- Reseller of open switches.

1 Gig-e switches:

- Edge-Core AS4600-54T
- Edge-Core AS4610-54T (HPE Altoline 6900)
- Quanta T1048-LB9
- Netberg Aurora 220

10 Gig-e switches:

- Edge-Core AS5610-52X
- Edge-Core AS5710-54X
- Edge-Core AS5712-54X (HPE Altoline 6920)
- Quanta T3048-LY2
- Quanta T3048-LY2R
- Quanta T3048-LY8
- Quanta T3048-LY9

25 Gig-e switches:

- Netberg Aurora 620

40 Gig-e switches:

- Edge-Core AS6700-32X
- Edge-Core AS6701-32X
- Edge-Core AS6712-32X (HPE Altoline 6940)
- Quanta T5032-LY6

100 Gig-e switches:

- Netberg Aurora 720
- Edge-Core AS7712-32X (HPE Altoline 6960)

All of the switches from Bare Metal Switches appear to use Broadcom ASICs. Broadcom contributed code to OpenCompute, which is an "Open Source" project, but what they include in github has a clearly non-free license:

https://github.com/Broadcom-Switch/OpenNSL/blob/master/Legal/LICENSE-Adv

"Licensee will not: Sell, rent, lease, distribute, sublicense, assign, or otherwise transfer (including by loan or gift) the Code".

I am disinclined to use Broadcom firmware:

https://web.archive.org/web/20080411030140/http://jebba.blagblagblag.org/?p=244

The switches they carry have a variety of CPUs: Freescale P2020 (PPC), Intel Atom, ARM.

The switches can run a variety of OSs, many non-free. They likely need non-free Broadcom firmware regardless of the OS (including ONL).

- OpenNSL – Broadcom chipsets. Accton. Github archive has proprietary license (LICENSE-Adv = non-free).
- OF-DPA – From Broadcom.
- SAI

4.4.3 Colfax Direct

- Website:
  http://www.colfaxdirect.com/
- Switches:
  http://www.colfaxdirect.com/store/pc/viewCategories.asp?idCategory=7

Colfax Direct sells a variety of HPC gear, including bare metal switches. They have network cards and other bits.

4.4.4 Penguin Computing

- Website:
  http://www.penguincomputing.com/

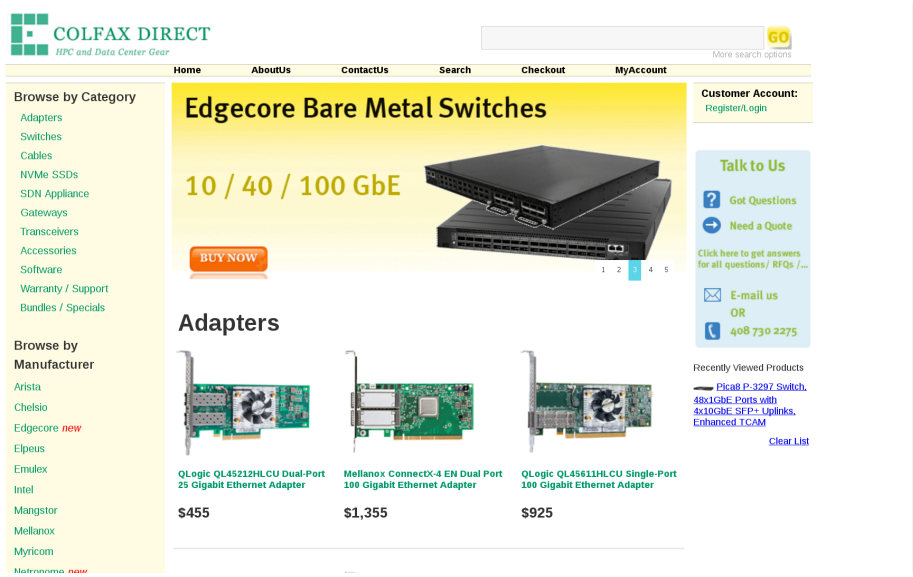

Figure 4.17: Colfax Direct Website

Slow manual order/quote process.

OS

Free Operating Systems

There are a lot of operating systems to consider to use as a firewall...

5.1 Requirements

Notes on some requirements in a firewall.

- Must be free software.
- The project must still be alive.
- Does it use a hardened kernel?
- How does it do security updates?
- Are there open security issues?
- Are there any CVEs?
- How are security issues handled?
- Is there a list of security issues?
- Does it have a wifi portal? (Should that be a separate box or in OpenWRT?)
- Does upstream https actually work?
- UTM - Unified Threat Management (e.g. snort, etc.)
- Load balancing between multiple upstreams (without BGP).
- Load balancing between dual local routers.
- Fail over to standby router (e.g. pfsync).
- "Anti-virus", SMTP, POP scans? Meh? (e.g. OpenBSD has greylist/tarpit.)
- Packet cleansing (e.g. tcp header randomization).
- Do we want DNS, DHCP, etc? Probably not?
- OpenVPN (built into router, or thru it?).

- Network graphing (MRTG, aguri, etc.)
- No broken "community" editions.
- Have mirrored server doing analysis?
- NAT options? cone, etc.
- Local system monitoring (e.g. system temp, hdd status, etc.)
- sshd
- GSM, pppd ?
- Two-factor authentication.
- snort, suricata

5.2 Firewall Operating Systems in Use

5.2.1 Debian

Debian

Aleph Objects uses Debian for nearly everything. It could easily be used as a router/firewall. There are better, more tuned options.

Linux's iptables is used on servers.

5.2.2 pfSense

pfSense

pfSense is used for the main firewalls. See pfSense chapter for more info. A few notes from the initial test install:

- Released May 18th, 2016.
- pfSense-CE-memstick-2.3.1-RELEASE-amd64.img
- FreeBSD 10.3 based.
- Installer feels like a step back in computing history.
- First boot goes to console with lots of useful options.

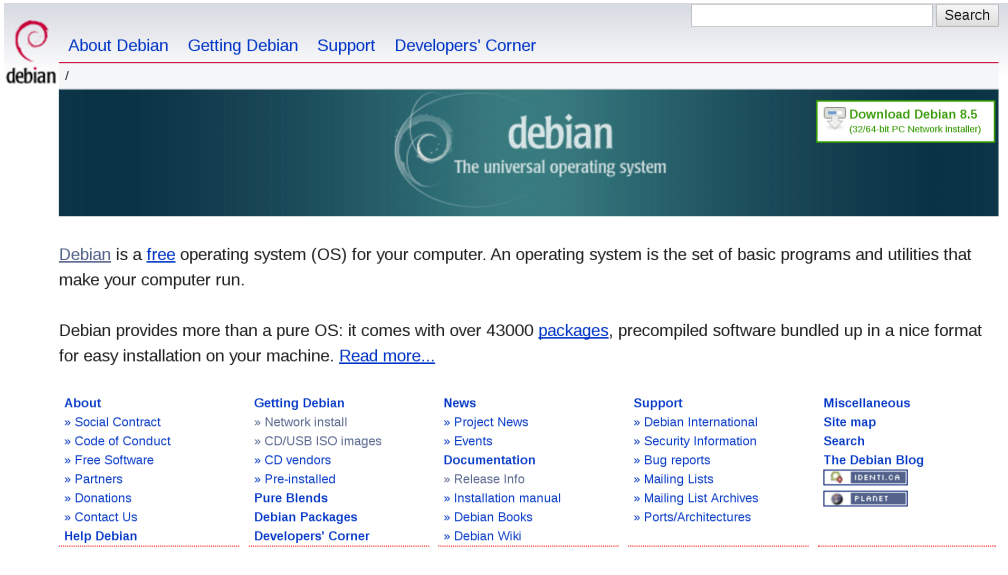

Figure 5.1: Debian Website

- Web admin wizard mentions pfSense Gold Subscriptions. It doesn't appear to be for non-free software (e.g. isn't baitware).
- They sell very nice looking hardware with pfsense pre-installed. With failover systems (CARP).
- Load balancing, failover.
- Clean and very responsive web interface (based on Bootstrap).
- Web based updater to new minor version.
- x86 architecture only.
- Looks to have good security errata process, following FreeBSD.
- Snort threat lists are available. Paid for more recent ones, same as on other snort platforms.
- Installation of additional packages is clean, and doesn't appear to offer any non-free.
- ClamAV ...

5.2.3 FreeBSD

FreeBSD

FreeBSD is used as the base for pfSense.

Figure 5.2: FreeBSD Website

Solid OS. Can use OpenBSD's PF (packet filtering). Same problem as with OpenBSD, few admins know it.

5.3 Firewalls Evaluated

The following firewalls were installed and tested for evaluation. pfSense was selected over these due to it being Free Software, its high security, the vast feature set, regular maintenance, and just being glorious overall.

5.3.1 pfSense

A few notes from the initial pfSense test install:

- Released May 18th, 2016.
- pfSense-CE-memstick-2.3.1-RELEASE-amd64.img

- FreeBSD 10.3 based.
- Installer feels like a step back in computing history.
- First boot goes to console with lots of useful options.
- Web admin wizard mentions pfSense Gold Subscriptions. It doesn't appear to be for non-free software (e.g. isn't baitware).
- They sell very nice looking hardware with pfsense pre-installed. With failover systems (CARP).
- Load balancing, failover.
- Clean and very responsive web interface (based on Bootstrap).
- Web based updater to new minor version.
- x86 architecture only.
- Looks to have good security errata process, following FreeBSD.
- Snort threat lists are available. Paid for more recent ones, same as on other snort platforms.
- Installation of additional packages is clean, and doesn't appear to offer any non-free.
- ClamAV ...

5.3.2 Alpine Linux

Alpine — "Small. Simple. Secure. Alpine Linux is a security-oriented, lightweight Linux distribution based on musl libc and busybox."

Download and install .iso to USB. Boot from USB, do text install onto HD. The installer looked very much like OpenBSD and was quite terse, but worked fine. The installed system is a basic lean GNU/Linux installation. Firewall configuration is text based. Looks nice, but not many features, except lightweight. Similar to OpenWRT in that way, except no web GUI, AFAICT.

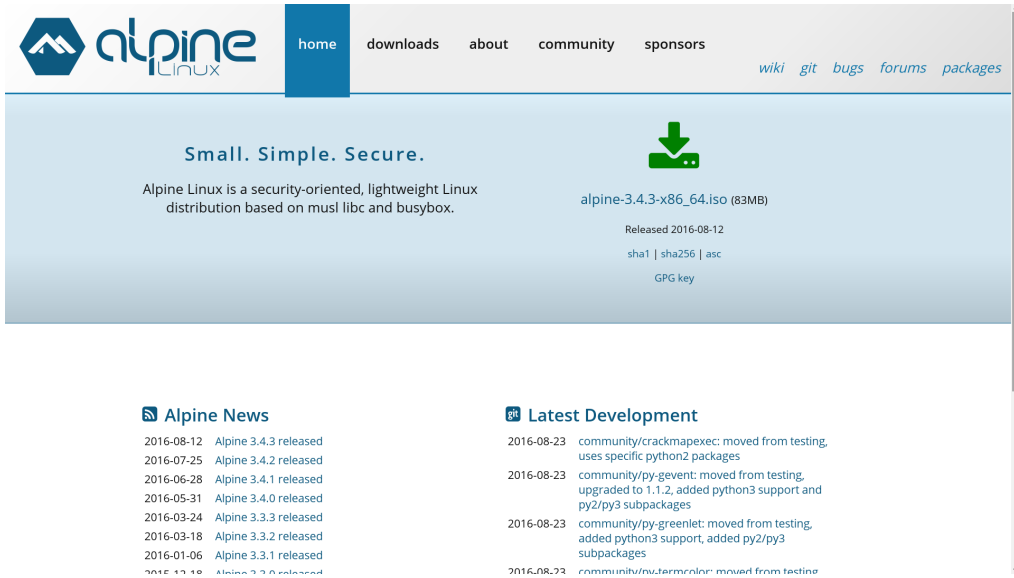

Figure 5.3: Alpine Linux Website

5.3.3 clearOS

clearOS — "ClearOS is an operating system for your Server, Network, and Gateway systems. It is designed for homes, small to medium businesses, and distributed environments. ClearOS is commonly known as the Next Generation Small Business Server, while including indispensable Gateway and Networking functionality. It delivers a powerful IT solution with an elegant user interface that is completely web-based."

- Overall, very very nice, very clean with many features.
- Baitware is the only thing holding this back.
- The web interface never crashed or caused issues.
- Usage is stable.
- Latest release: 7.2.0
- Release Date: March 7, 2015.
- Package Updater: yum

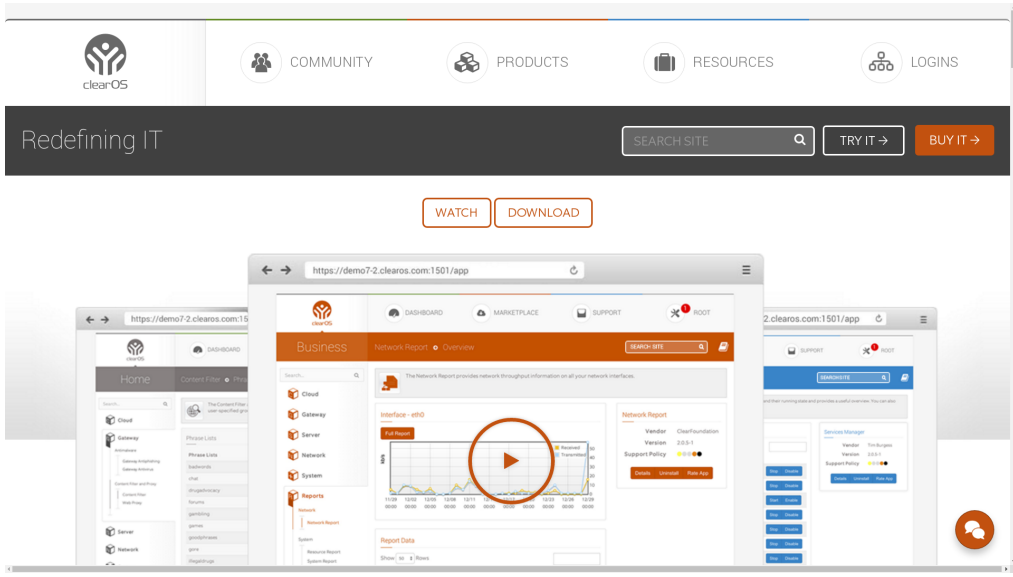

Figure 5.4: clearOS Website

- Kernel: Linux 3.10.0-327.3.1.el17.x86_64
- Base OS: Fedora? CentOS?
- Easy GUI install
- Has enterprise (baitware?) version.
- Has enterprise hardware.
- Web based configuration system started on first boot
- Web wizard has option to select Community or non-free versions.
- Web wizard has system registration for a marketplace for apps. Have to register?
- Registering set “Software End-of-Life” to August 31, 2018.
- Lots of phone-home activity with marketplace and registration....
- Simple “Update All” button to update system (with yum, afaict).

- Very clean, overall.
- Wide variety of "Apps" in the Marketplace that are GPL.
- Non-free plugins are listed along free ones. The owncloud plugin is non-free.
- Most apps don't have any ratings.
- The default "Exception Sites" whitelist had their clear*.com sites and a few *.microsoft.com.
- Has optionally transparent web proxy.
- Installed many Apps, and it was all very clean.
- clearOS gets pwned, we get pwnd? Yes.
- Need to create account to get to knowledge base ?
- Actual firewalling rules (e.g. block just these devices from everything but port 443) aren't so strong.
- There doesn't appear to be a way to say "just allow port 22 from NNN"...
- A lot of great setup.
- MultiWAN — Nice, but simple load balancing between multiple upstreams.
- Failover to multiple upstreams.
- No fail over to another router (ala CARP).
- dhclient (?) overwrites DNS addresses, no place to set static (?!?)
- Some pretty graphs, but not the most useful.
- Overall kind of a toy compared to pfSense.

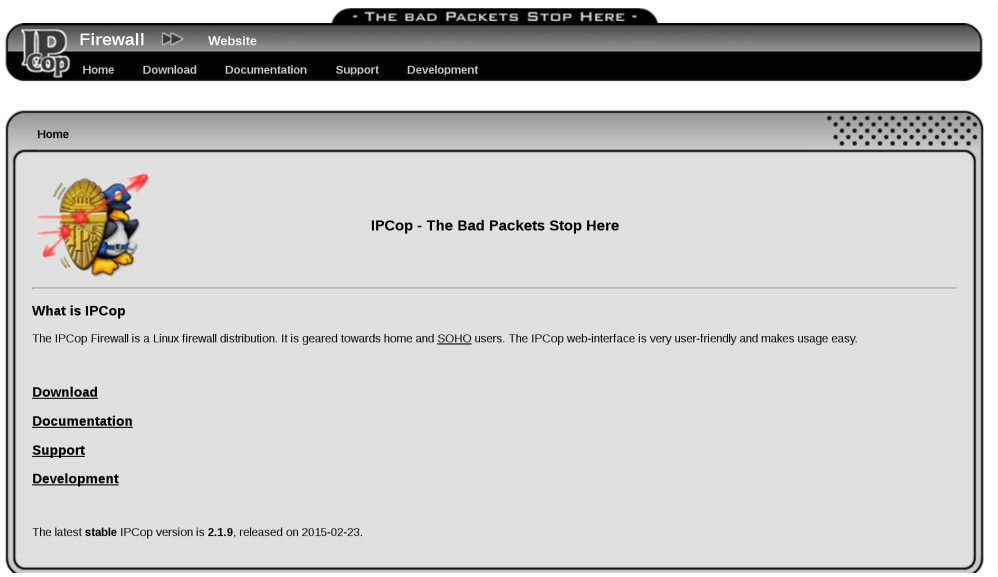

Figure 5.5: IPCop Website

5.3.4 IPCop

IPCop — "The IPCop Firewall is a Linux firewall distribution. It is geared towards home and SOHO users. The IPCop web-interface is very user-friendly and makes usage easy."

- Last release was 2015-02-23, well over a year ago.
- The i486 image doesn't boot all the way, gives video artifacts.
- All looks pretty old and crufty at this point.

5.3.5 IPFire

IPFire — "the professional and hardened Linux firewall distribution that is secure, easy to operate and coming with great functionality so that it is ready for enterprises, authorities, and anybody else."

- Latest release: July 12th, 2016.
- `http://downloads.ipfire.org/releases/ipfire-2.x/2.19-core103/ipfire-2.19.x86_64-full-core103.iso`

Figure 5.6: IPFire Website

- Installer has a cool thing that flashes the light on the ethernet port to identify it.
- Kernel: Linux 3.14.65-ipfire
- Post install, apache httpd process is starting, but not listening on any ports. Still in "-k start". So no web admin. Needed to modify listen.conf in Apache to 0.0.0.0:80 and 0.0.0.0:444. It appears it was hanging because of IPv6 (?).
- Nice MRTG-esque graphs of services and ports, including system temps, etc.
- Second set of non-MRTG network traffic graphs.
- Transparent web caching.
- Much more technical setup than clearOS. More SysAdmin oriented.
- OpenVPN.
- QoS.

- Load balancing? Fail over?
- IDS (snort).
- Uses its own pakfire package management tool.
- The wiki is under an NC license.
- Kernel uses grsec.
- No WAN failover (!).

5.3.6 OPNsense

OPNsense — "the Open Source Firewall that is easy-to-use and protects your network"

Figure 5.7: OPNsense Website

- Release is current.
- Making a dd of the .iso to a USB drive didn't boot. OPNsense-16.7.r2-OpenSSL-cdrom-amd64.iso

- Based on FreeBSD.
- Source in github.
- Looks decent, but wasn't tested.

5.4 Previous Operating Systems in Use

5.4.1 OpenBSD

OpenBSD

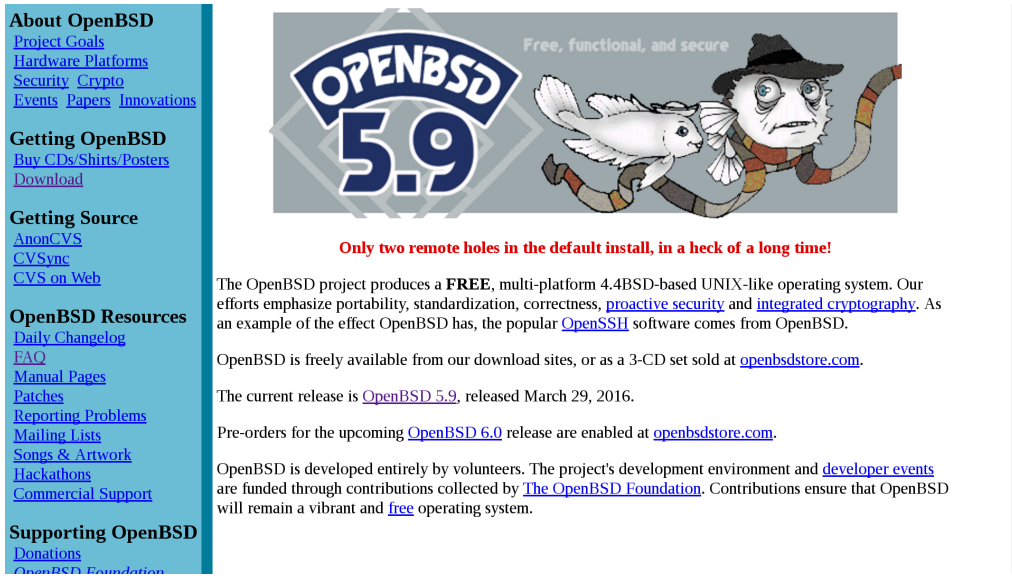

Figure 5.8: OpenBSD Website

Aleph Objects has dropped OpenBSD in favor of pfSense.

OpenBSD with PF was previously used for our firewall for the first five years. It is very reliable and secure. Few people know how to administer it. It is all command line editing of firewall configuration files.

5.5 Other

5.5.1 Gentoo

Gentoo
: Can be tuned in.

5.5.2 NetBSD

NetBSD
: Solid OS. Can use OpenBSD's pf, iirc. Same problem as with OpenBSD, few admins know it.

Contact

Phone, Email, Web, Location

6.1 Support

Email: `support@alephobjects.com`
Phone: +1-970-377-1111 x610

6.2 Sales

Email: `sales@alephobjects.com`
Phone: +1-970-377-1111 x600

6.3 Website

Aleph Objects, Inc.
`www.alephobjects.com`

Colophon

Created with 100% Free Software

Debian GNU/Linux

LaTeX Memoir