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.

20160826

Contents

List of Figures

Introduction

Firewall

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.

Firewall

Stop.

1.1 Overview

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

1.2 iptables

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

Figure 1.1: Netfilter Website

1.3 pfSense

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.

Figure 1.2: pfSense Website

1.3.1 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.

1.3.2 Traffic Shaping

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

1.3.3 pfBlockerNG

- IP blocklists for botnets, etc.

1.3.4 Suricata

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

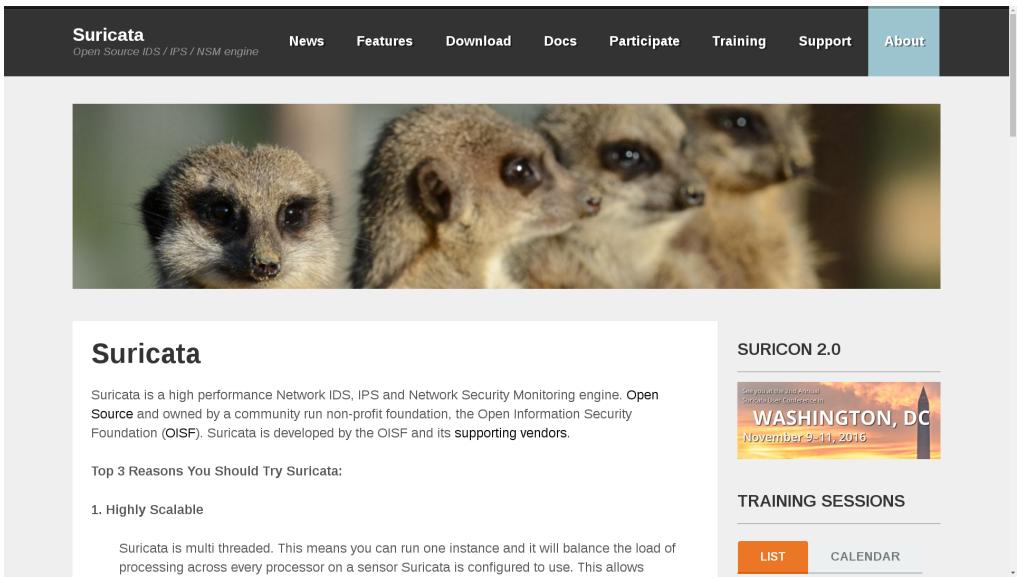

Figure 1.3: Suricata Website

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

1.3.5 DHCP

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

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

1.3.6 NTP

1.3.7 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."

Figure 1.4: OpenVPN Website

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

1.3.8 Captive Portal

The Captive Portal for Aleph Mountain building wifi services.

1.3.9 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.

1.3.10 ssh

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

1.3.11 DNS

DNS forwarding is provided by Dnsmasq.

1.3.12 Routing

- No BGP, OSPF, etc.
- Static backbone routes.
- WAN failover

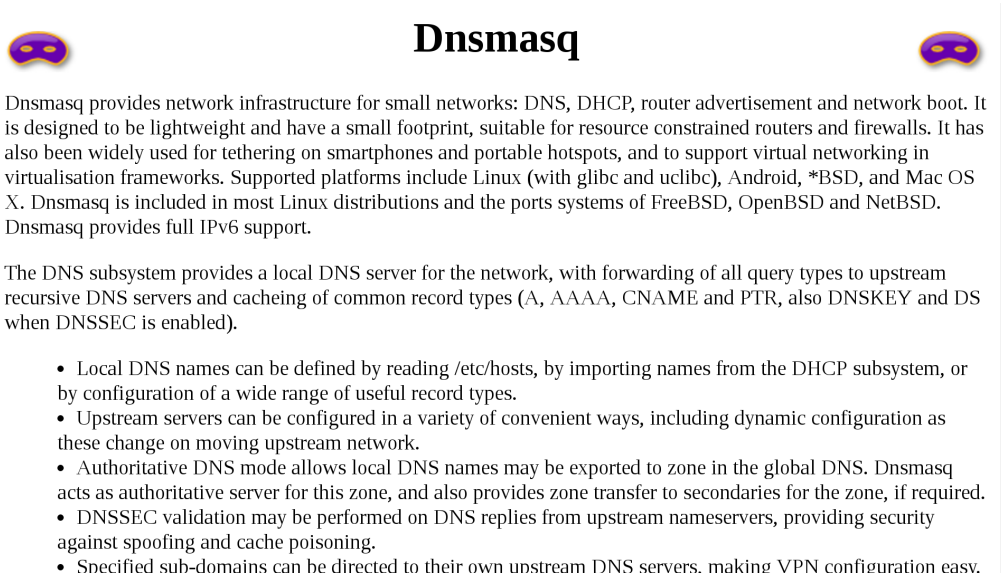

Figure 1.5: Dnsmasq Website

1.3.13 Interfaces

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

1.3.14 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.

1.3.15 Reporting

- Dashboard.
- Darkstat.

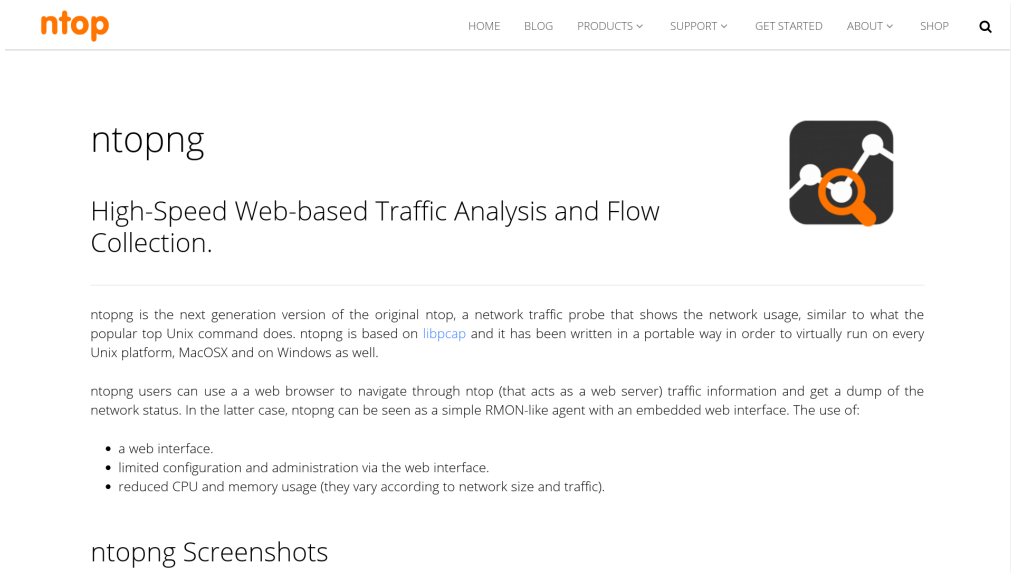

Figure 1.6: ntopng Website

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

1.3.16 Install notes

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.

- 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 ...

Hardware

Purchase Order

2.1 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.

3.1 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.

3.2 Free Software for Network Switches

3.2.1 ONIE

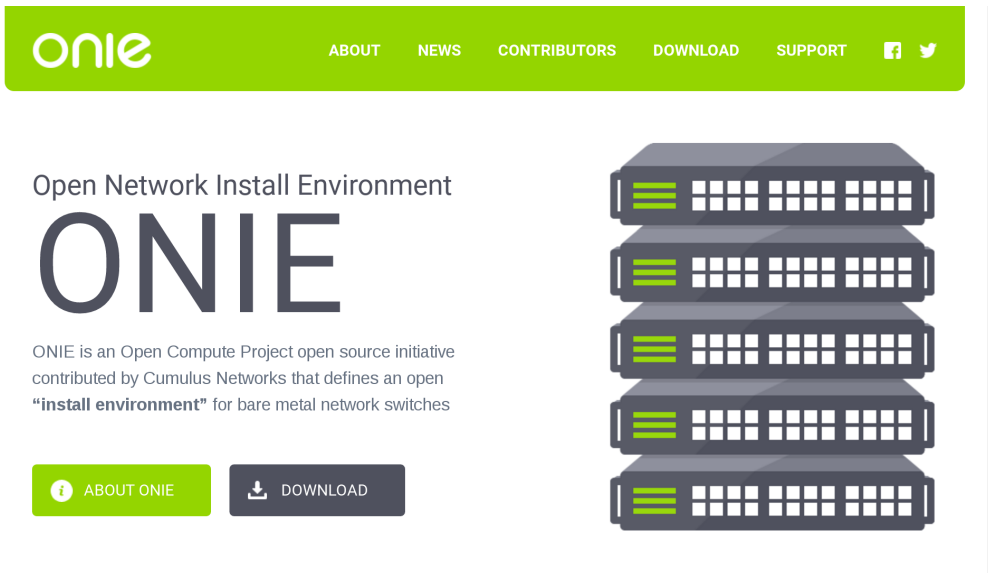

Figure 3.1: ONIE Website

- 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."

3.2.2 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

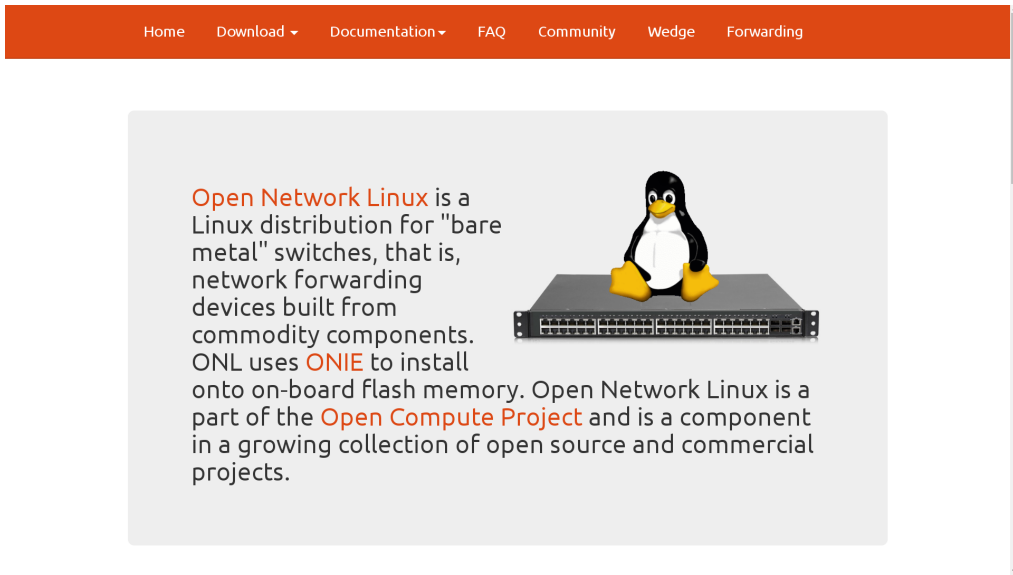

Figure 3.2: Open Network Linux Website

- 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"

3.2.3 Snaproute

- aka OpenSnaproute, FlexSwitch.

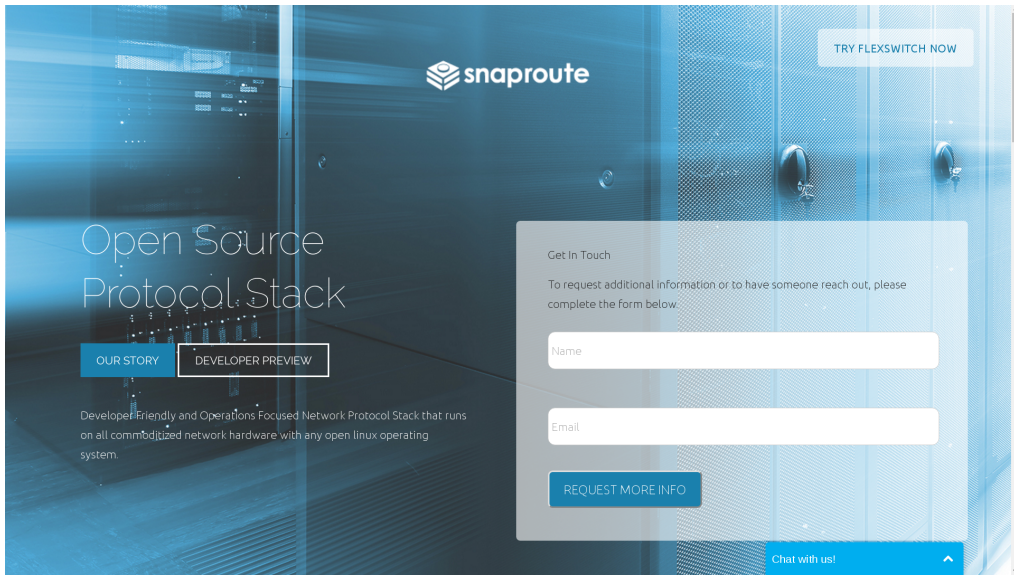

Figure 3.3: Snaproute Website

- 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."

3.2.4 OpenSwitch

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

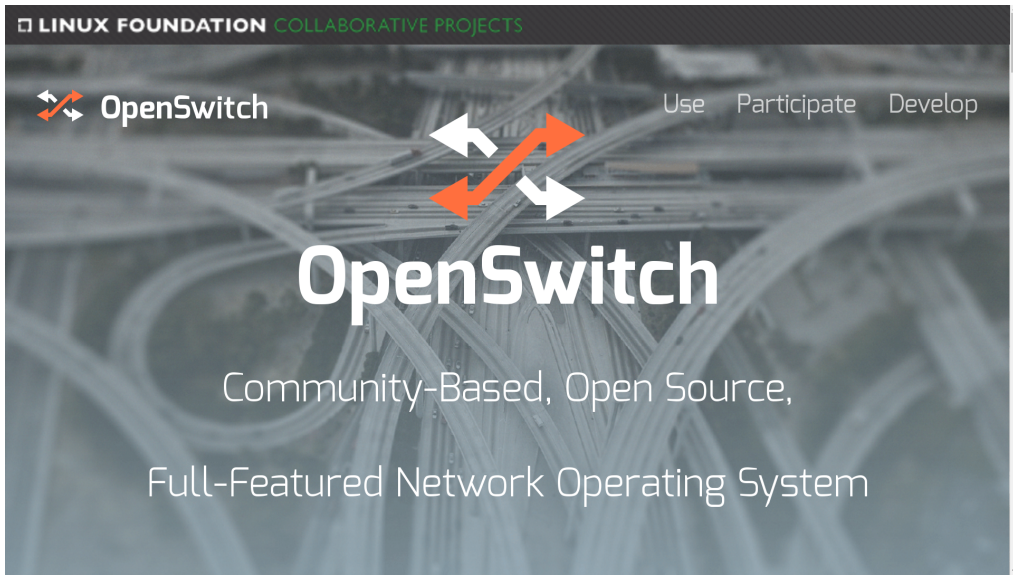

Figure 3.4: OpenSwitch Website

"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.

3.2.5 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.

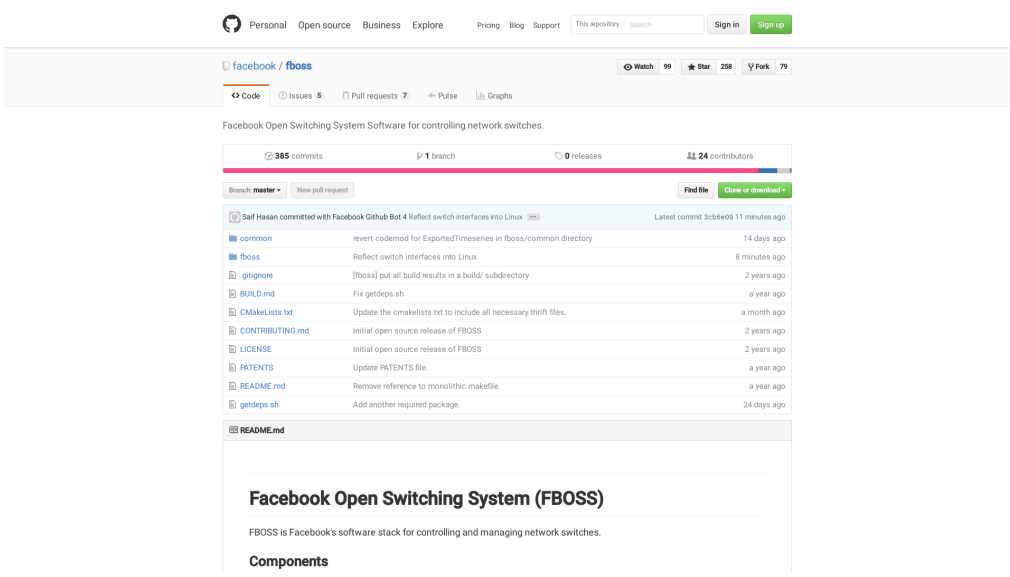

Figure 3.5: FBOSS Website

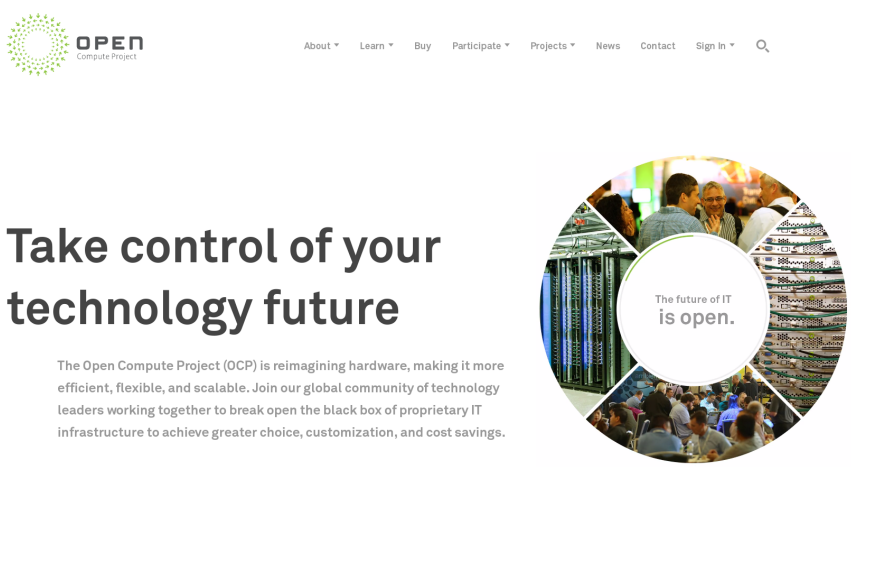

Figure 3.6: OpenCompute Website

3.2.6 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.

3.2.7 Big Switch

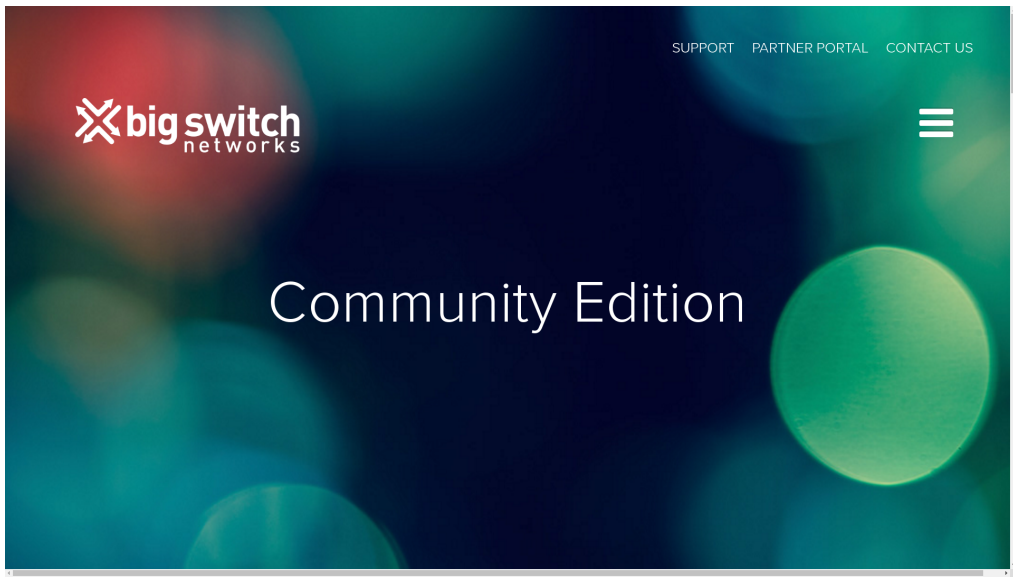

Figure 3.7: Big Switch Website, no

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

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

3.2.8 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...

3.3 Hardware

Hardware, on which to place free software.

3.3.1 Edge-Core

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

3.3.2 Dell

- Website:
  http://dell.com/

Dell makes some bare metal switches that are ONIE compatible.

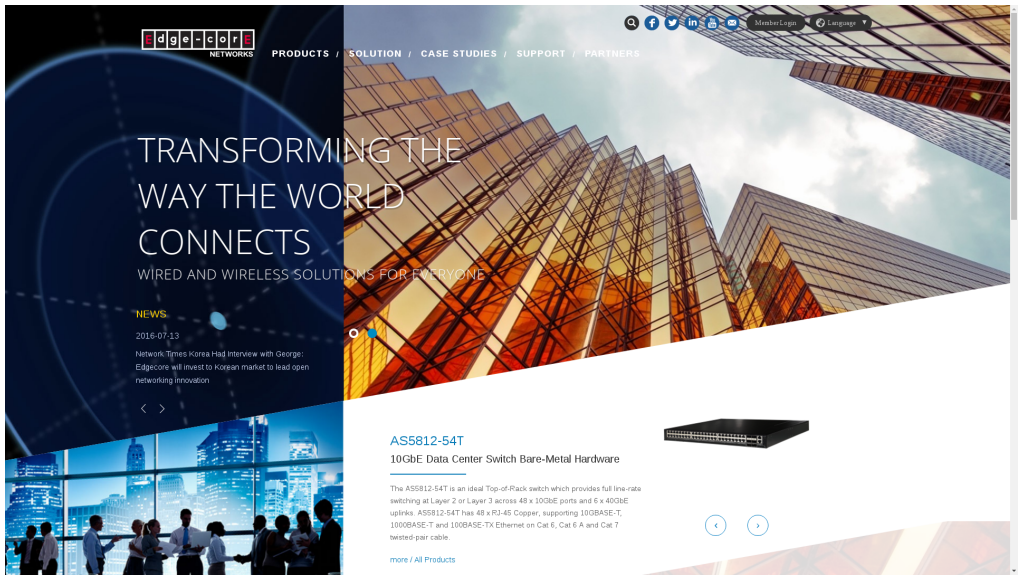

Figure 3.8: Edge-core Website

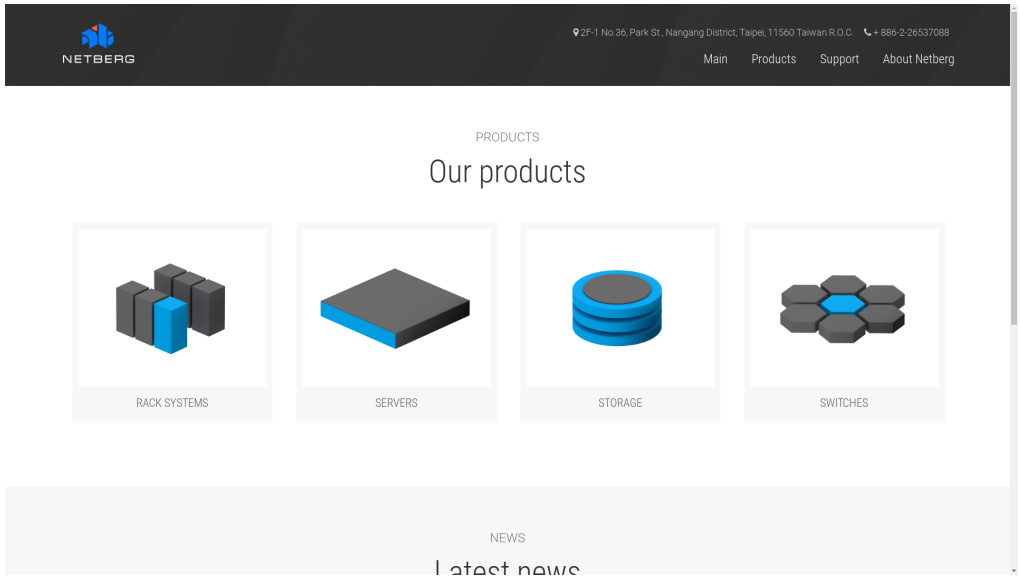

Figure 3.9: Netberg Website

3.3.3 Netberg

- Website:
  http://netbergtw.com/

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

3.3.4 Quanta

Figure 3.10: Quanta Website

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

Uses...Broadcom.

Figure 3.11: Mellanox Website

3.3.5 Mellanox

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

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

3.4 Suppliers

3.4.1 White Box

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

1 Gig-e switches available:

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

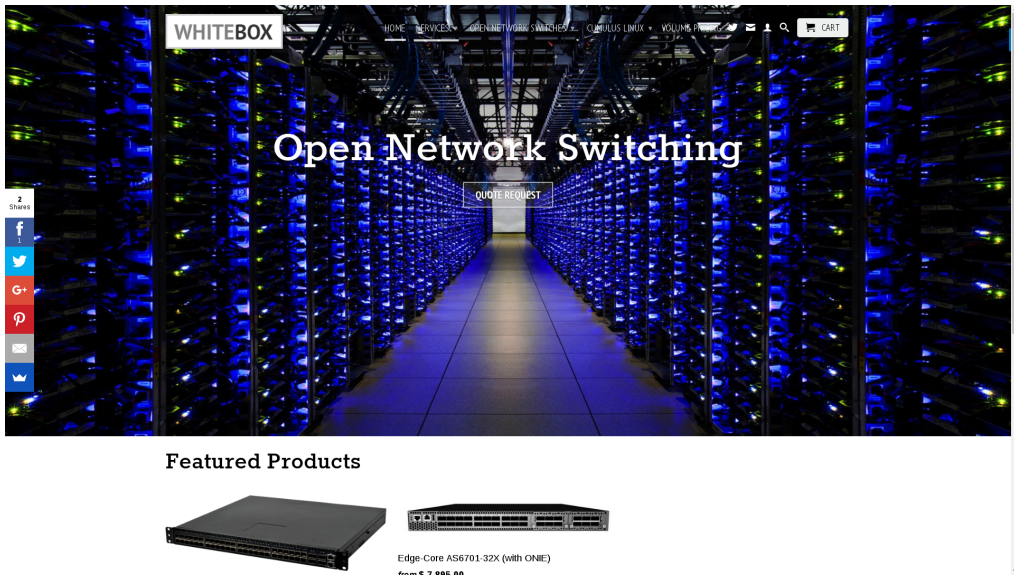

Figure 3.12: Whitebox Website

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.

3.4.2 Bare Metal Switches

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

1 Gig-e switches:

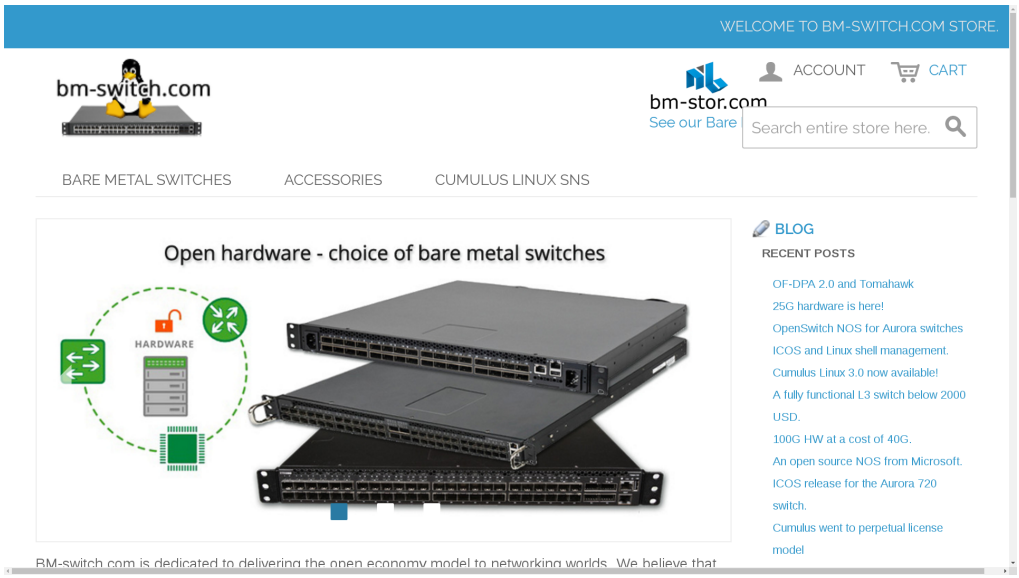

Figure 3.13: Bare Metal Switches Website

- 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

3.4.3 Colfax Direct

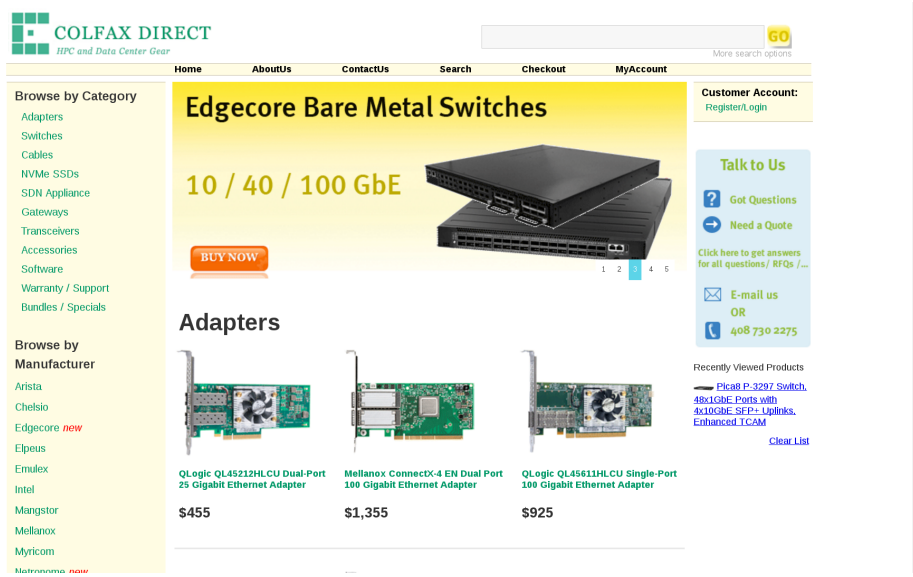

Figure 3.14: Colfax Direct Website

- 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.

3.4.4 Penguin Computing

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

Slow manual order/quote process.

OS

Free Operating Systems

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

4.1 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

4.2 Firewall Operating Systems in Use

4.2.1 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.

4.2.2 pfSense

pfSense

pfSense is used for the main firewalls. See pfSense chapter for more info.

4.2.3 FreeBSD

FreeBSD

FreeBSD is used as the base for pfSense.

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

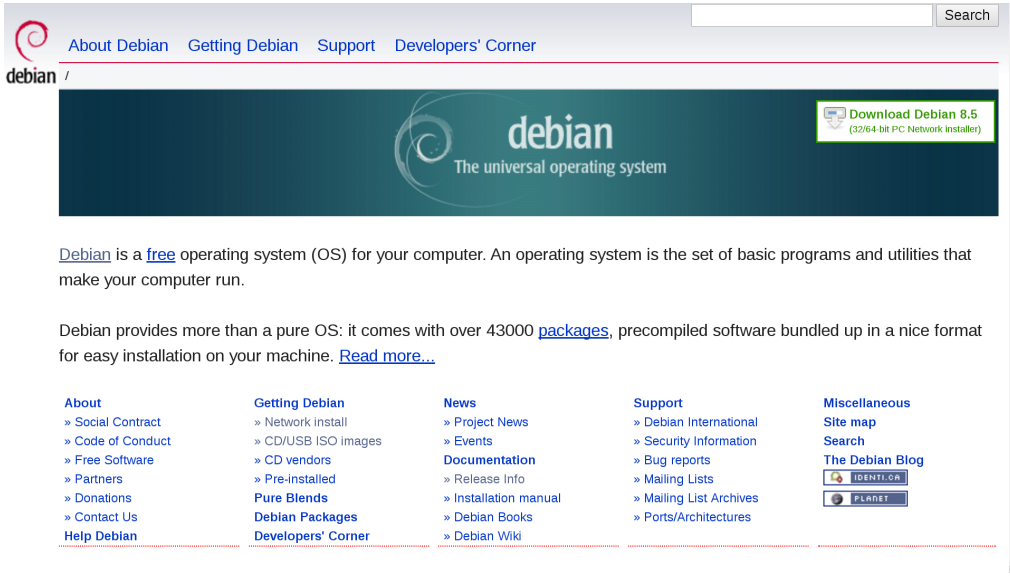

Figure 4.1: Debian Website

Figure 4.2: FreeBSD Website

4.3 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.

4.3.1 Alpine Linux

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

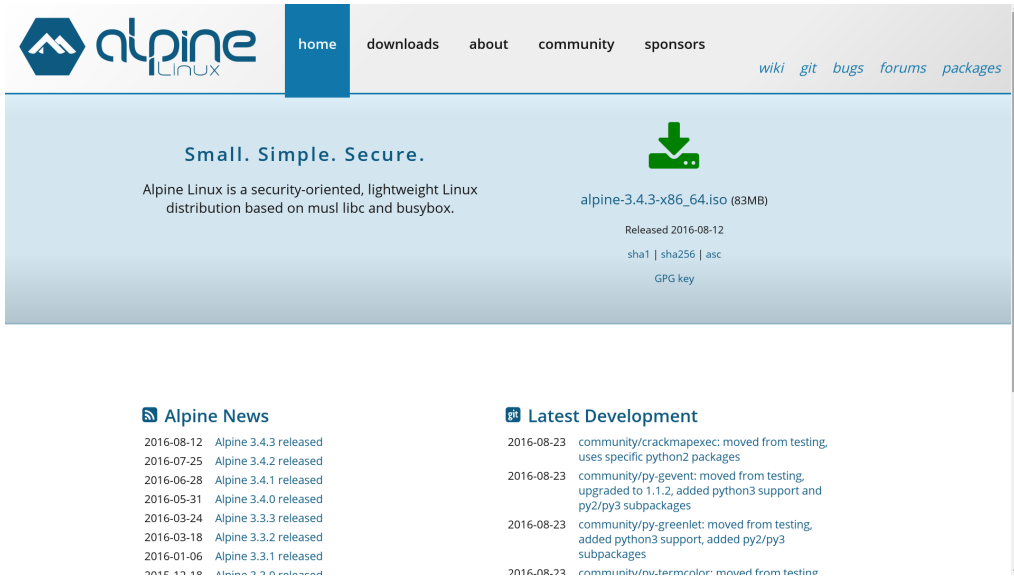

Figure 4.3: Alpine Linux Website

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.

4.3.2 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."

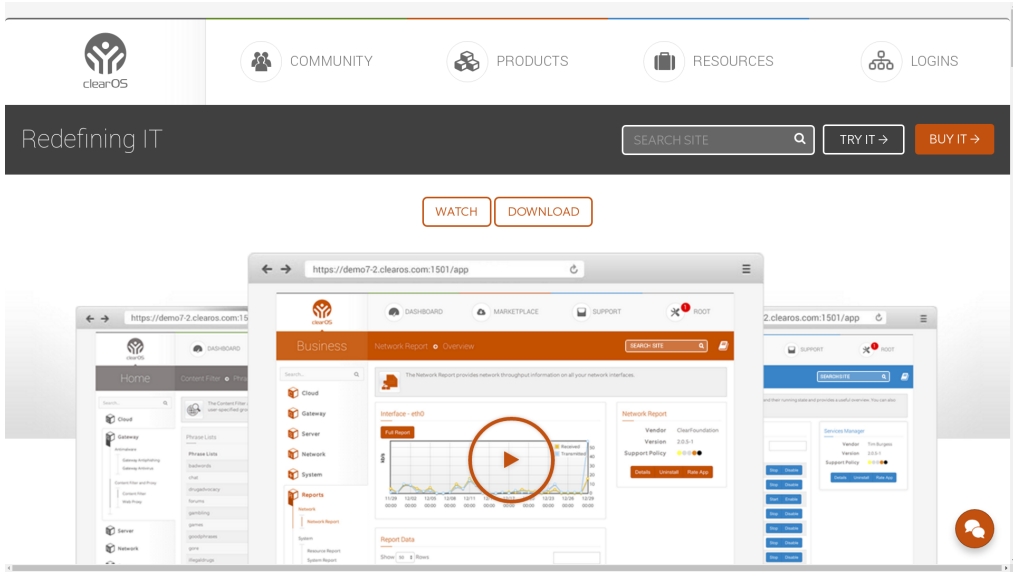

Figure 4.4: clearOS Website

- 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

- 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.

4.3.3 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.

4.3.4 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`

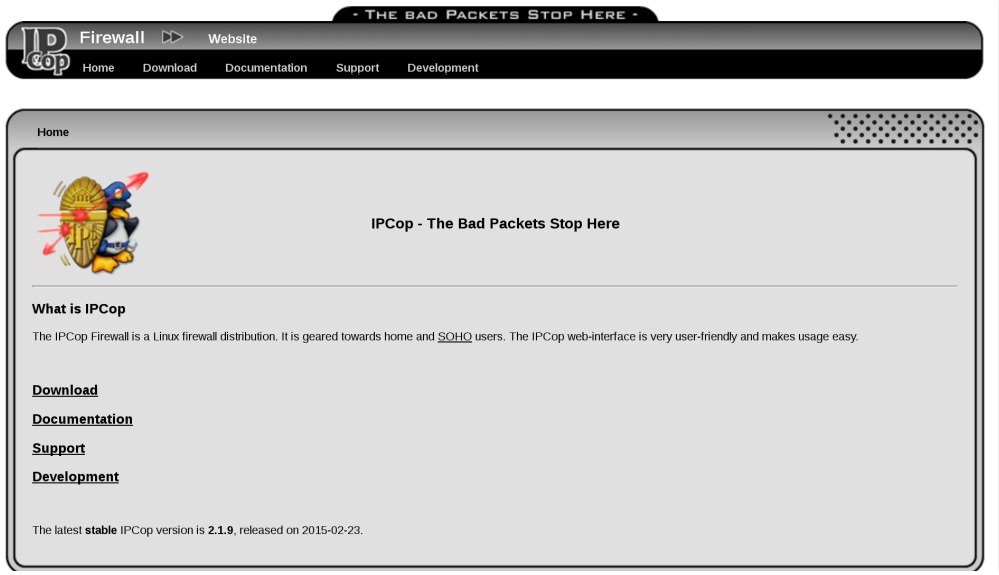

Figure 4.5: IPCop Website

Figure 4.6: 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 (!).

4.3.5 OPNsense

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

- 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.

Figure 4.7: OPNsense Website

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

4.4 Previous Operating Systems in Use

4.4.1 OpenBSD

OpenBSD

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.

4.5 Other

4.5.1 Gentoo

Gentoo

Figure 4.8: OpenBSD Website

Can be tuned in.

4.5.2 NetBSD

NetBSD

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

Contact

Phone, Email, Web, Location

5.1 Support

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

5.2 Sales

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

5.3 Website

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

Colophon

Created with 100% Free Software

Debian GNU/Linux

LaTeX Memoir