



**ALEPH
OBJECTS[®]**
INCORPORATED

FIREWALL

Aleph Objects Firewall

by Aleph Objects, Inc.

Copyright © 2014, 2015, 2016 Aleph Objects, Inc.

**Permission is granted to copy, distribute and/or modify this document
under the terms of the Creative Commons Attribution 4.0 International
Public License (CC BY-SA 4.0).**

**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.

20160902

Contents

Introduction	
Firewall	vii
1 Firewall	
Stop.	9
1.1 Overview	10
1.2 iptables	10
1.3 pfSense	10
1.3.1 Configuration	11
1.3.2 NAT	15
1.3.3 Traffic Shaping	15
1.3.4 pfBlockerNG	16
1.3.5 Suricata	16
1.3.6 DHCP	17
1.3.7 NTP	17
1.3.8 OpenVPN	17
1.3.9 Captive Portal	18
1.3.10 SSL Certificates	18
1.3.11 ssh	18
1.3.12 DNS	19
1.3.13 Routing	19
1.3.14 Interfaces	19
1.3.15 CARP and Synchronization	20
1.3.16 Reporting	20
1.3.17 Test Evaluation Install notes	21
2 Hardware	
Purchase Order	23
2.1 Overview	24

CONTENTS

3 Switches Here.	25
3.1 Overview	26
3.2 Free Software for Network Switches	26
3.2.1 ONIE	26
3.2.2 Open Network Linux	27
3.2.3 Snaproute	28
3.2.4 OpenSwitch	29
3.2.5 FBOSS	30
3.2.6 Open Compute Project	32
3.2.7 OpenDataPlane	32
3.2.8 OpenFastPath	33
3.2.9 Open vSwitch	34
3.2.10 Big Switch	35
3.2.11 Uncategorized Software	35
3.3 Hardware	36
3.3.1 Edge-Core	36
3.3.2 Dell	36
3.3.3 Netberg	37
3.3.4 Quanta	37
3.3.5 Mellanox	38
3.4 Suppliers	39
3.4.1 White Box	39
3.4.2 Bare Metal Switches	40
3.4.3 Colfax Direct	42
3.4.4 Penguin Computing	42
4 OS	
Free Operating Systems	45
4.1 Requirements	46
4.2 Firewall Operating Systems in Use	47
4.2.1 Debian	47
4.2.2 pfSense	47
4.2.3 FreeBSD	47
4.3 Firewalls Evaluated	49
4.3.1 Alpine Linux	49
4.3.2 clearOS	50
4.3.3 IPCop	52

CONTENTS

4.3.4	IPFire	52
4.3.5	OPNsense	54
4.4	Previous Operating Systems in Use	55
4.4.1	OpenBSD	55
4.5	Other	55
4.5.1	Gentoo	55
4.5.2	NetBSD	56
5	Contact	
	Phone, Email, Web, Location	57
5.1	Support	58
5.2	Sales	58
5.3	Website	58

List of Figures

1.1	Netfilter Website	10
1.2	pfSense Website	11
1.3	Suricata Website	16
1.4	OpenVPN Website	17
1.5	Dnsmasq Website	19
1.6	ntopng Website	20
3.1	ONIE Website	26
3.2	Open Network Linux Website	28
3.3	Snaproute Website	29
3.4	OpenSwitch Website	30
3.5	FBOSS Website	31
3.6	OpenCompute Website	31
3.7	OpenDataPlane Website	32
3.8	OpenFastPath Website	33
3.9	Open vSwitch Website	34
3.10	Big Switch Website, no	35
3.11	Edge-core Website	36
3.12	Netberg Website	37
3.13	Quanta Website	38
3.14	Mellanox Website	38
3.15	Whitebox Website	39
3.16	Bare Metal Switches Website	40
3.17	Colfax Direct Website	43
4.1	Debian Website	48
4.2	FreeBSD Website	48
4.3	Alpine Linux Website	49
4.4	clearOS Website	50
4.5	IPCop Website	53
4.6	IPFire Website	53
4.7	OPNsense Website	55
4.8	OpenBSD Website	56

Introduction

Firewall

Introduction

This document at present is a rough collection of notes of different hardware and software evaluated 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.

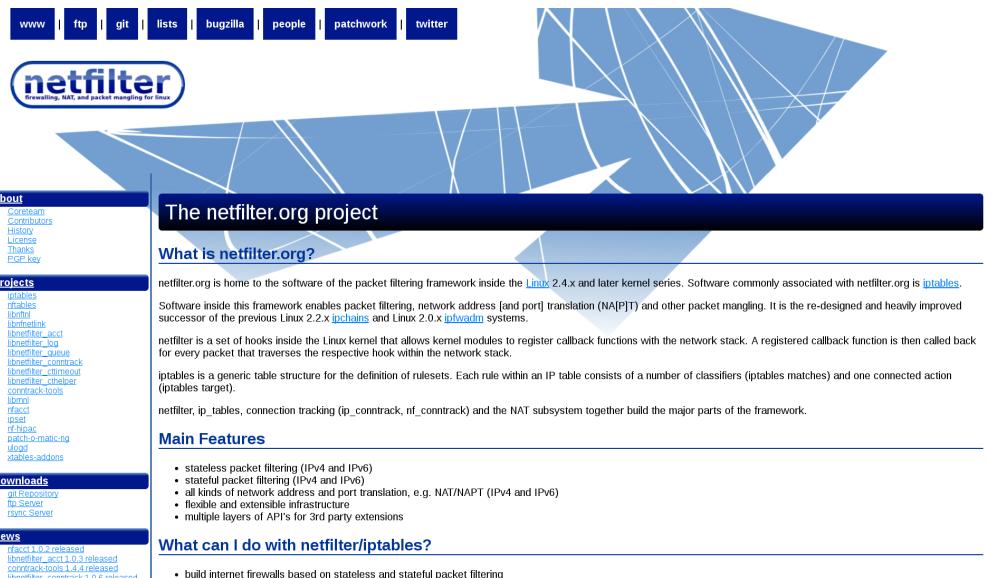


Figure 1.1: Netfilter Website

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.

1.3. PFSENSE

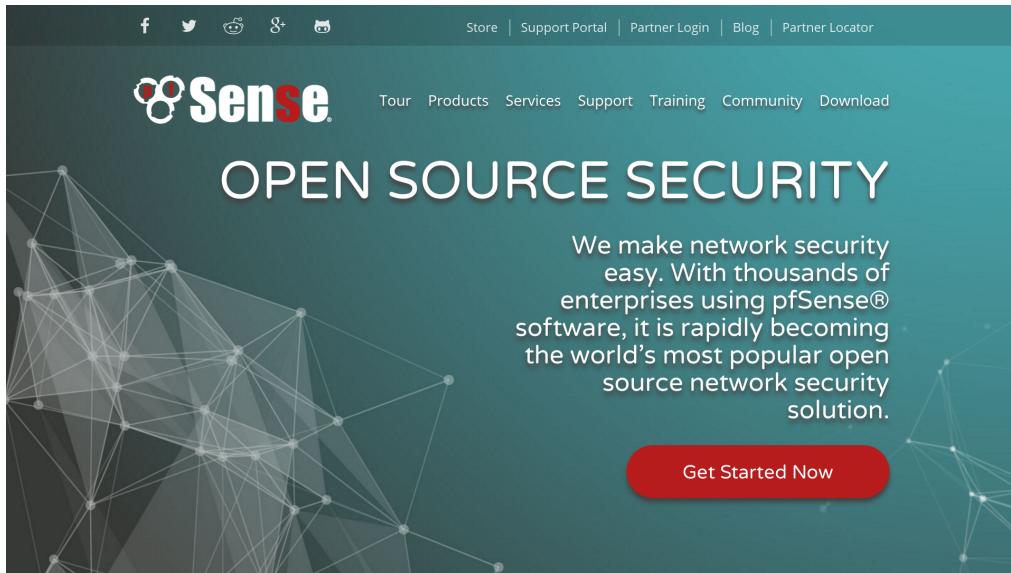


Figure 1.2: pfSense Website

1.3.1 Configuration

These are the the initial configuration steps for a pfSense firewall.

1. Connect via USB cable. 115200 baud, 8N1, no flow control.
2. Copy MAC address to main DHCP/DNS server, and reserve IP address.
3. Set IP for LAN (e.g. 192.168.1.1)
4. Set IP for WAN, disable IPv6
5. Log in to firewall (e.g. <https://192.168.1.1>). Initial pass admin/pfsense.
6. Start Wizard, hit Next.
7. pfSense Gold, Next.
8. Hostname: set hostname.
9. Set WAN, LAN, password, etc.

10. Hit Reload, and the wizard is done.
11. 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).
12. Log out and log back in as newly created user.
13. 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.
14. At this point, you can optionally SSH into the firewall if a key was set up for the user.
15. 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.
16. 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.
17. System → Notifications. Check for Disable Growl Notifications and Disable SMTP. Save.
18. System → Cert. Manager. Under Certificates, click Add. Method: Create a Certificate Signing Request. Descriptive Name, use the

1.3. PFSENSE

- hostname of the firewall being setup. Key length 4096, Digest Algorithm sha512. Country Code US, etc. Common name, use hostname of firewall. Save.
19. 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).
 20. 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.
 21. 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.
 22. System → Cert. Manager, also import any of our own CAs and Certificate Revocations, if any.
 23. 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.
 24. To use the newly set up certificate. System → Advanced, Admin Acess. Change SSL Certificate to the new one. Save. Now go to that new hostname with https and the correct port.
 25. 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.

26. 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.
27. 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.
28. 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.
29. 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...
30. 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.
31. Diagnostics -> Backup & Restore. Backup.
32. Diagnostics -> Reboot and make sure everything comes up clean.
33. 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 do 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..
34. System -> Routing. Click to edit the mini pencil icon on the Gateway line listed as Default. Monitor IP: something appropriate upstream,

1.3. PFSENSE

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.

35. System → Update, System Update. Check that the Status is “Up to date.” If it needs updating, update.
36. 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.
37. System → Package Manager, Available Packages. Install: Cron, ntopng, openvpn-client-export, pfBlockerNG, RRD_Summary, Status_Traffic_Totals, sudo, suricata.
38. System → sudo. Add user, optionally.
39. OpenVPN setup.
40. Interfaces → LAN. When you’re done using the LAN as any sort of gateway. Change IPv4 Upstream gateway to None. Save. Apply Changes.
41. Diagnostics → Backup & Restore. Backup.
42. Diagnostics → Reboot and make sure everything comes up clean.

1.3.2 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.

1.3.3 Traffic Shaping

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

1.3.4 pfBlockerNG

- IP blocklists for botnets, etc.

1.3.5 Suricata

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

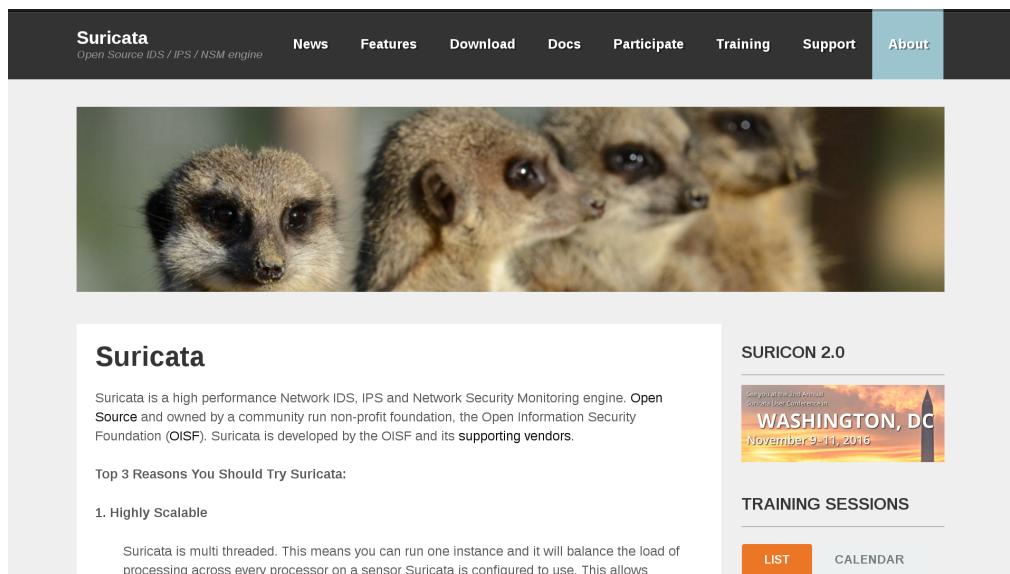


Figure 1.3: Suricata Website

- barnyard2
- Snort Blacklists

1.3. PFSENSE

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

1.3.6 DHCP

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

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

1.3.7 NTP

1.3.8 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.
- Mobiles.
- SSL certificates.



Figure 1.4: OpenVPN Website

- 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
```

1.3.9 Captive Portal

The Captive Portal for Aleph Mountain building wifi services.

1.3.10 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.

1.3.11 ssh

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

1.3.12 DNS

DNS forwarding is provided by Dnsmasq.

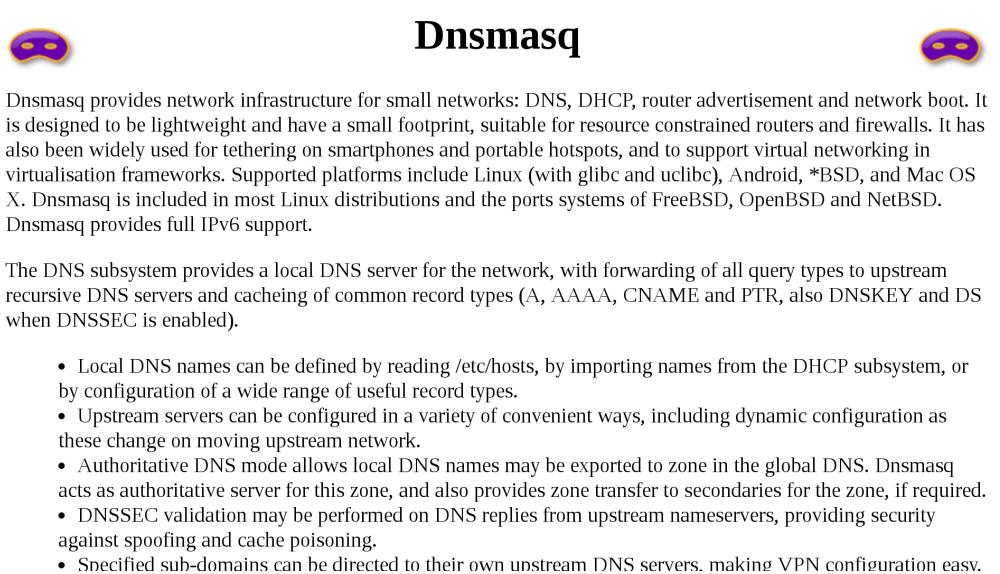


Figure 1.5: Dnsmasq Website

1.3.13 Routing

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

1.3.14 Interfaces

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

1.3.15 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.

1.3.16 Reporting

ntop

HOME BLOG PRODUCTS ▾ SUPPORT ▾ GET STARTED ABOUT ▾ SHOP 

ntopng

High-Speed Web-based Traffic Analysis and Flow Collection.

ntopng is the next generation version of the original ntop, a network traffic probe that shows the network usage, similar to what the popular top Unix command does. ntopng is based on [libpcap](#) and it has been written in a portable way in order to virtually run on every Unix platform, Mac OSX and on Windows as well.

ntopng users can use a web browser to navigate through ntop (that acts as a web server) traffic information and get a dump of the network status. In the latter case, ntopng can be seen as a simple RMON-like agent with an embedded web interface. The use of:

- a web interface.
- limited configuration and administration via the web interface.
- reduced CPU and memory usage (they vary according to network size and traffic).

ntopng Screenshots

Figure 1.6: ntopng Website

- Dashboard.

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

1.3.17 Test Evaluation 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.

Firewall

- 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

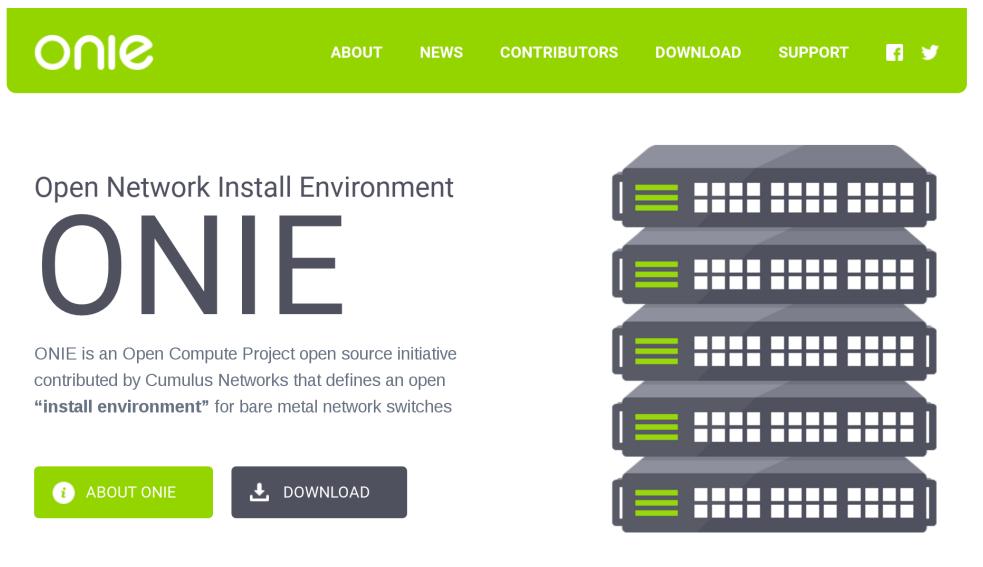


Figure 3.1: ONIE Website

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

3.2. FREE SOFTWARE FOR NETWORK SWITCHES

- 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

The screenshot shows the homepage of the Open Network Linux website. At the top, there is a red navigation bar with links: Home, Download ▾, Documentation ▾, FAQ, Community, Wedge, and Forwarding. Below the navigation bar, there is a large white area containing text and an image. On the left, the text describes Open Network Linux as a "bare metal" switch distribution built from commodity components, using ONIE for installation. On the right, there is a small illustration of Tux, the Linux mascot, sitting on top of a network switch.

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.

3.2. FREE SOFTWARE FOR NETWORK SWITCHES

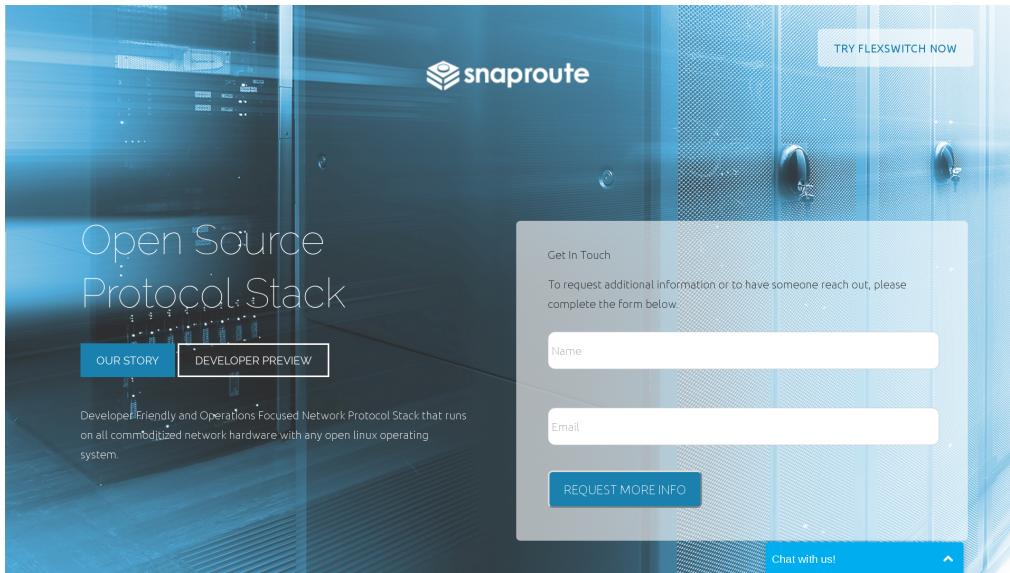


Figure 3.3: Snaproute Website

- 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 compatibility 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.

3.2. FREE SOFTWARE FOR NETWORK SWITCHES

The screenshot shows the GitHub repository page for 'facebook / fboss'. At the top, there are links for Personal, Open source, Business, Explore, Pricing, Blog, Support, and a search bar. Below the header, the repository name 'facebook / fboss' is displayed, along with statistics: 385 commits, 1 branch, 0 releases, and 24 contributors. A green button labeled 'Close & download' is visible. The main content area shows a list of commits from 'Saf Hasan' with details like commit messages and timestamps. Below the commit list, there's a section titled 'Facebook Open Switching System (FBOSS)' with a brief description: 'FBOSS is Facebook's software stack for controlling and managing network switches.' A 'Components' section is also present.

Figure 3.5: FBOSS Website

The screenshot shows the Open Compute Project (OCP) website. At the top, there's a navigation bar with links for About, Learn, Buy, Participate, Projects, News, Contact, Sign In, and a search icon. The main heading is 'Take control of your technology future'. Below it, a subtext reads: 'The Open Compute Project (OCP) is reimagining hardware, making it more efficient, flexible, and scalable. Join our global community of technology leaders working together to break open the black box of proprietary IT infrastructure to achieve greater choice, customization, and cost savings.' To the right, there's a circular graphic containing several smaller images related to technology and infrastructure, with the text 'The future of IT is open.' in the center.

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 OpenDataPlane

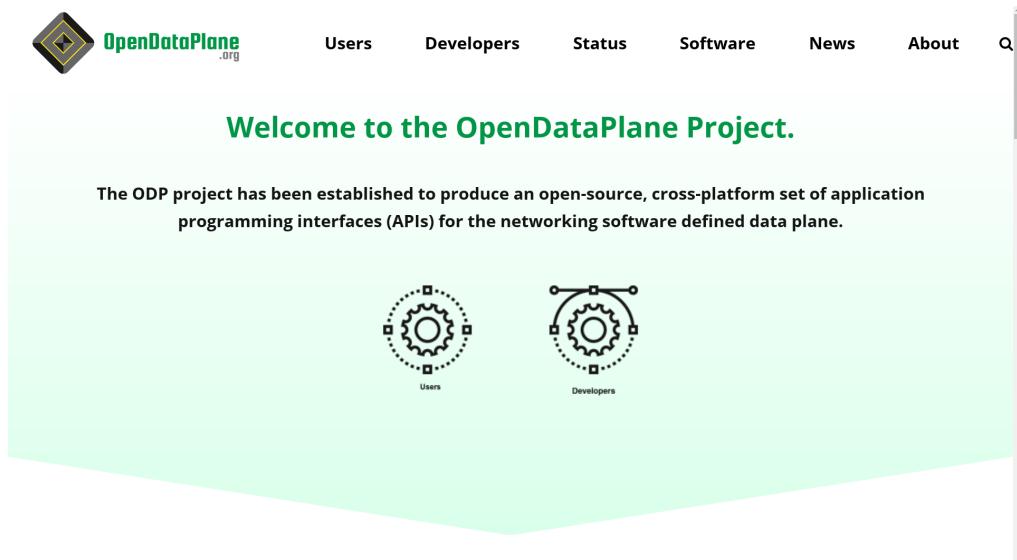


Figure 3.7: OpenDataPlane Website

- Website:
<http://opendataplane.org/>

3.2. FREE SOFTWARE FOR NETWORK SWITCHES

- 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/>

3.2.8 OpenFastPath

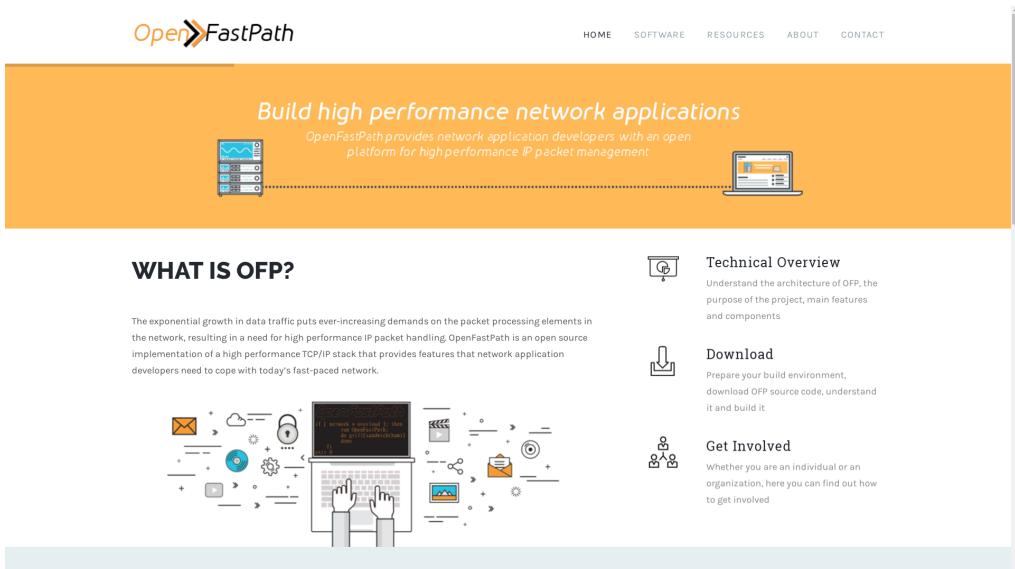


Figure 3.8: OpenFastPath Website

- 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.”

3.2.9 Open vSwitch



Figure 3.9: 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).”

3.2. FREE SOFTWARE FOR NETWORK SWITCHES

3.2.10 Big Switch



Figure 3.10: Big Switch Website, no

- Website:
<http://www.bigsswitch.com/community-edition>

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

3.2.11 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

Switches

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

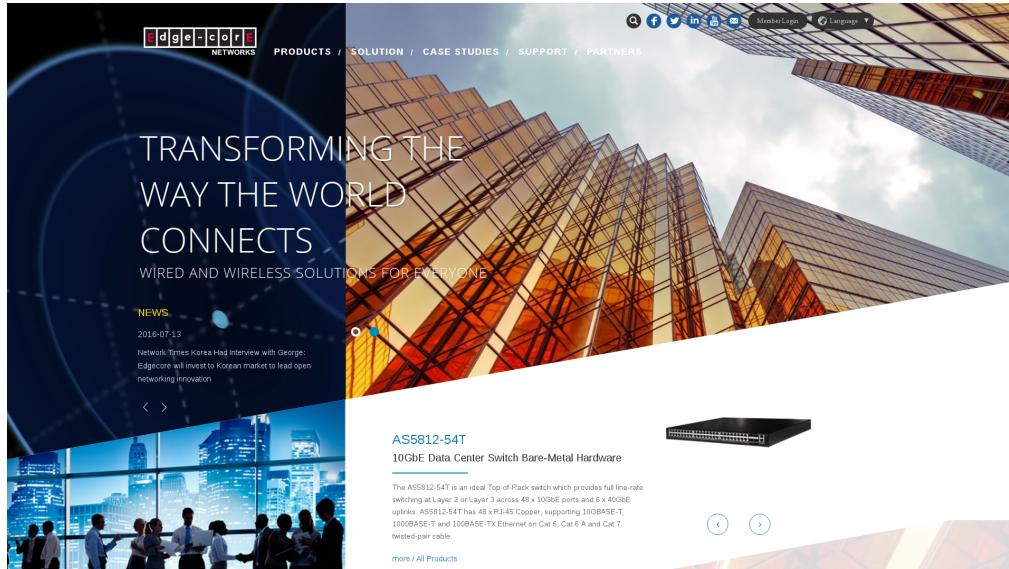


Figure 3.11: Edge-core Website

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

3.3.2 Dell

- Website:
<http://dell.com/>

3.3. HARDWARE

Dell makes some bare metal switches that are ONIE compatible.

3.3.3 Netberg

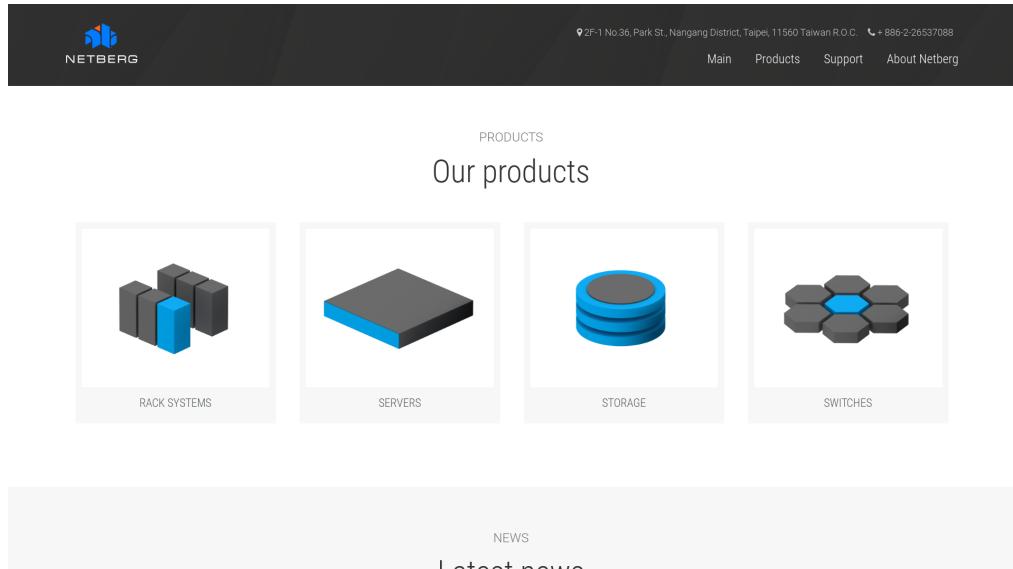


Figure 3.12: Netberg Website

- Website:
<http://netbergtw.com/>

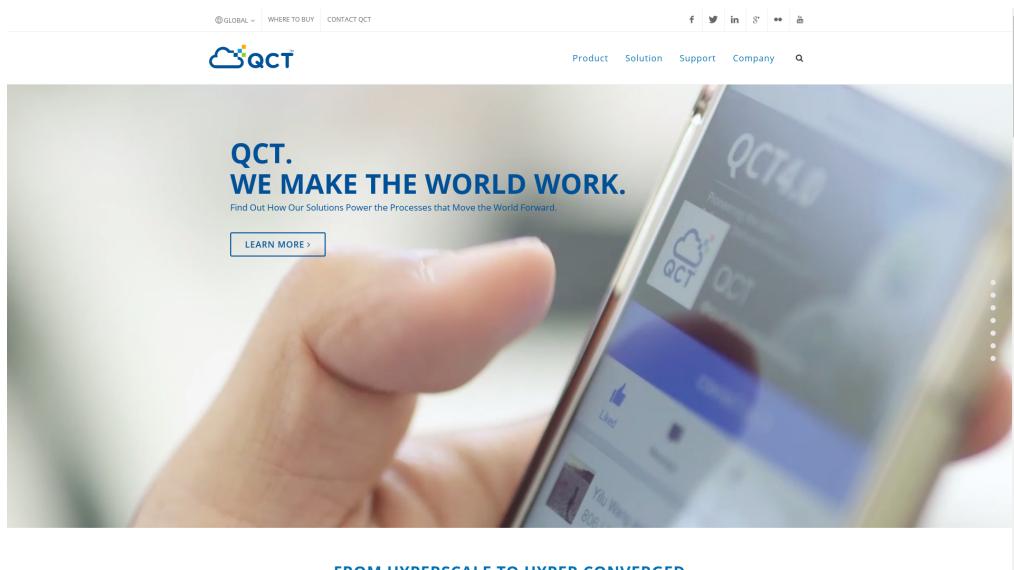
Netberg may be the manufacturer of some pfSense branded hardware.
Appears to be...Broadcom based...

3.3.4 Quanta

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

Uses...Broadcom.

Switches



FROM HYPERSCALE TO HYPER CONVERGED

Figure 3.13: Quanta Website

3.3.5 Mellanox



Figure 3.14: Mellanox Website

3.4. SUPPLIERS

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

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

3.4 Suppliers

3.4.1 White Box



Figure 3.15: Whitebox Website

- Website:
<http://whiteboxswitch.com/>

- Reseller of open switches.

1 Gig-e switches available:

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

Switches

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

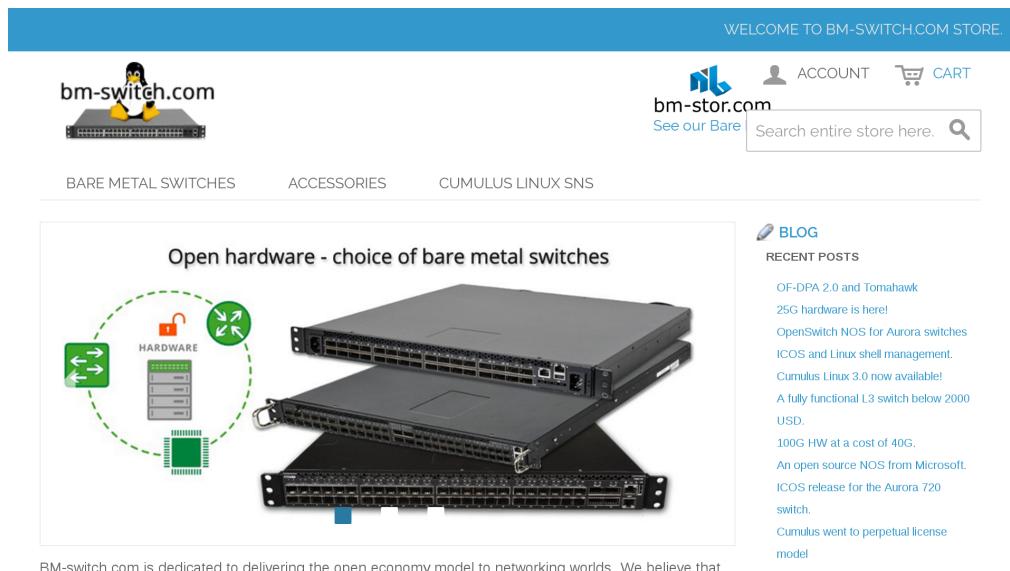


Figure 3.16: Bare Metal Switches Website

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

3.4. SUPPLIERS

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

3.4.3 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.

3.4.4 Penguin Computing

- Website:

<http://www.penguincomputing.com/>

3.4. SUPPLIERS

The screenshot shows the Colfax Direct website with the following details:

- Header:** COLFAX DIRECT HPC and Data Center Gear, Home, AboutUs, ContactUs, Search, Checkout, MyAccount, Go, More search options.
- Left Sidebar (Browse by Category):** Adapters, Switches, Cables, NVMe SSDs, SDN Appliance, Gateways, Transceivers, Accessories, Software, Warranty / Support, Bundles / Specials.
- Left Sidebar (Browse by Manufacturer):** Arista, Chelsio, Edgecore **new**, Elpues, Emulex, Intel, Mangstor, Mellanox, Myricom, Netronome **new**.
- Main Content:** Edgecore Bare Metal Switches, 10 / 40 / 100 GbE, BUY NOW button, two Edgecore switches shown.
- Bottom Content:** Adapters section with three network adapter cards:
 - QLogic QL45212HLCU Dual-Port 25 Gigabit Ethernet Adapter, \$455
 - Mellanox ConnectX-4 EN Dual Port 100 Gigabit Ethernet Adapter, \$1,355
 - QLogic QL45611HLCU Single-Port 100 Gigabit Ethernet Adapter, \$925
- Right Sidebar:** Customer Account: Register/Login, Talk to Us (Got Questions, Need a Quote), Click here to get answers for all questions/RFQs..., E-mail us OR 408 730 2275, Recently Viewed Products (Picot P-3292 Switch, 48x1GbE Ports with 4x10GbE SFP+ Uplinks, Enhanced TCAM), Clear List.

Figure 3.17: 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...

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?).

4.2. FIREWALL OPERATING SYSTEMS IN USE

- 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.

The screenshot shows the official Debian website. At the top, there's a navigation bar with links to "About Debian", "Getting Debian", "Support", and "Developers' Corner". Below this is a large banner featuring the Debian logo and the text "The universal operating system". To the right of the banner is a button labeled "Download Debian 8.5 (32/64-bit PC Network Installer)". The main content area contains text about Debian being a free operating system and provides links for installation and more information. A footer navigation bar at the bottom includes sections for "About", "Getting Debian", "News", "Support", and "Miscellaneous", along with links to "Social Contract", "Code of Conduct", "Free Software", "Partners", "Donations", "Contact Us", "Help Debian", "Documentation", "Installation manual", "Debian Books", "Debian Wiki", "Project News", "Events", "Release Info", "Bug reports", "Mailing Lists", "Mailing List Archives", "Ports/Architectures", "Debian International", "Security Information", "Search", "The Debian Blog", "IDENTI.ORA", and "PLANET".

Figure 4.1: Debian Website

The screenshot shows the official FreeBSD website. The header features the FreeBSD logo and the tagline "The Power To Serve". It includes a "Donate to FreeBSD" button, a search bar, and language selection links (de, en, es, fr, hu, it, ja, nl, ru, zh_CN). The main content area has a section titled "The FreeBSD Project" with a paragraph about FreeBSD's history and features, followed by links to "Learn More" and "Get the FreeBSD Journal". To the right is a cartoon character of a red devil-like creature holding a pitchfork. There's a yellow box for "Download FreeBSD" and another for "LATEST RELEASES" (Production: 10.3, 10.2, 10.1, 9.3; Upcoming: 11.0, Support Lifecycle). A "IPv6 Armenia" dropdown menu is also present. On the far right, there's a "SHORTCUTS" section with links to "Mailing Lists", "Reporting Problems", "FAQ", "Handbook", and "Ports". A "New to FreeBSD?" button is located in the bottom right corner.

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 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 ...

4.3.2 Alpine Linux

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

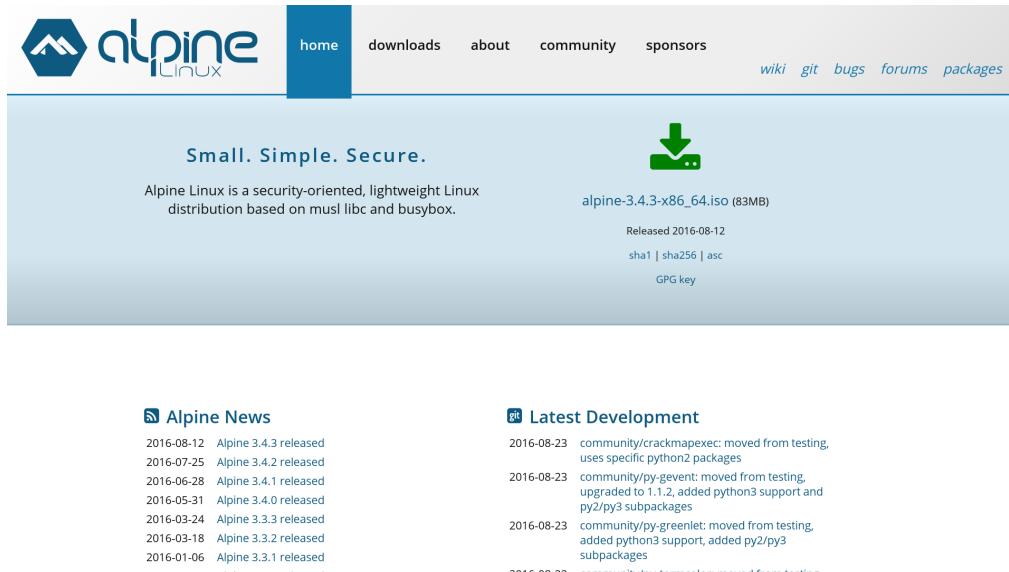


Figure 4.3: Alpine Linux Website

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.

4.3.3 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.”

4.3. FIREWALLS EVALUATED

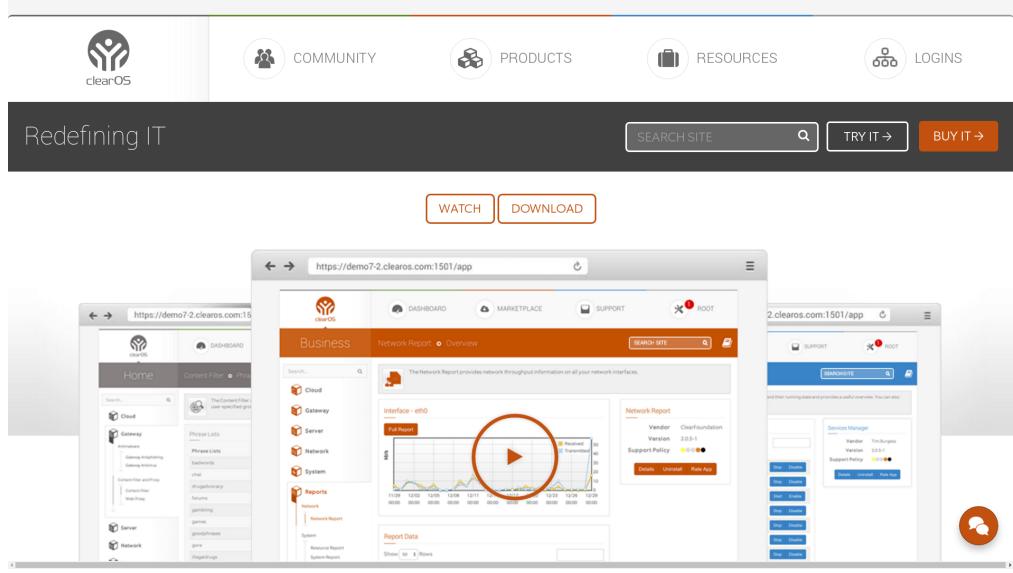


Figure 4.4: clearOS Website

- 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.

4.3. FIREWALLS EVALUATED

- 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.

4.3.4 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.”

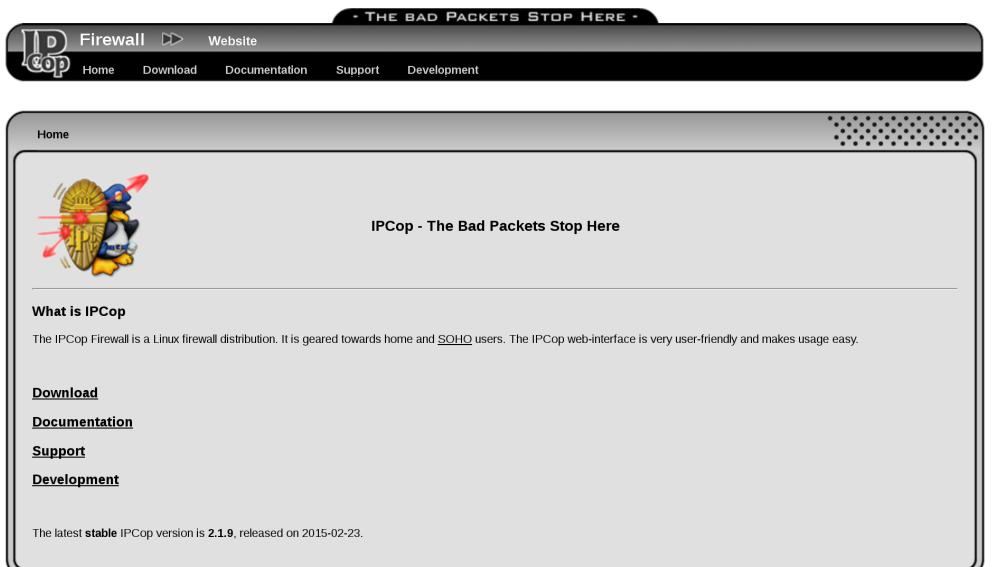


Figure 4.5: IPCop Website

- 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 crusty at this point.

4.3.5 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.”

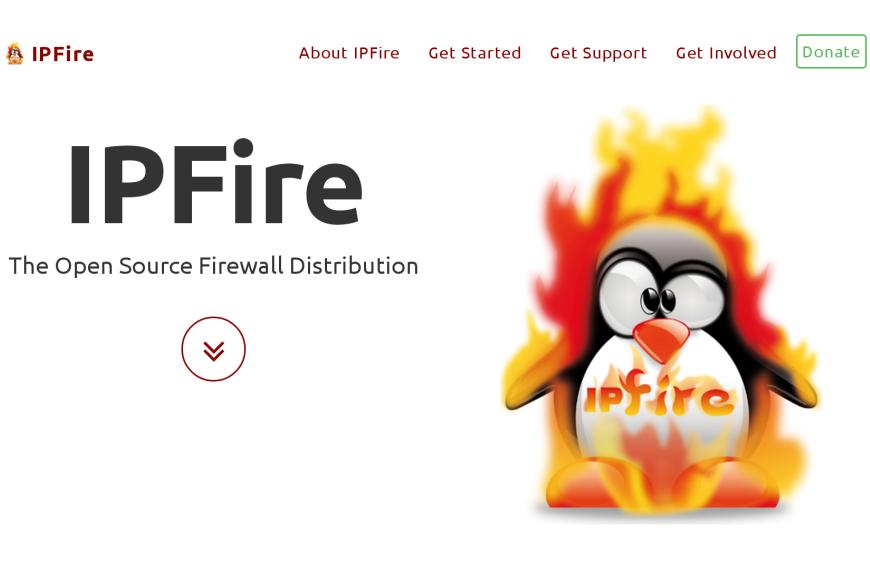


Figure 4.6: IPFire Website

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

4.3. FIREWALLS EVALUATED

- 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 (!).

4.3.6 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.
- Source in github.
- Looks decent, but wasn’t tested.

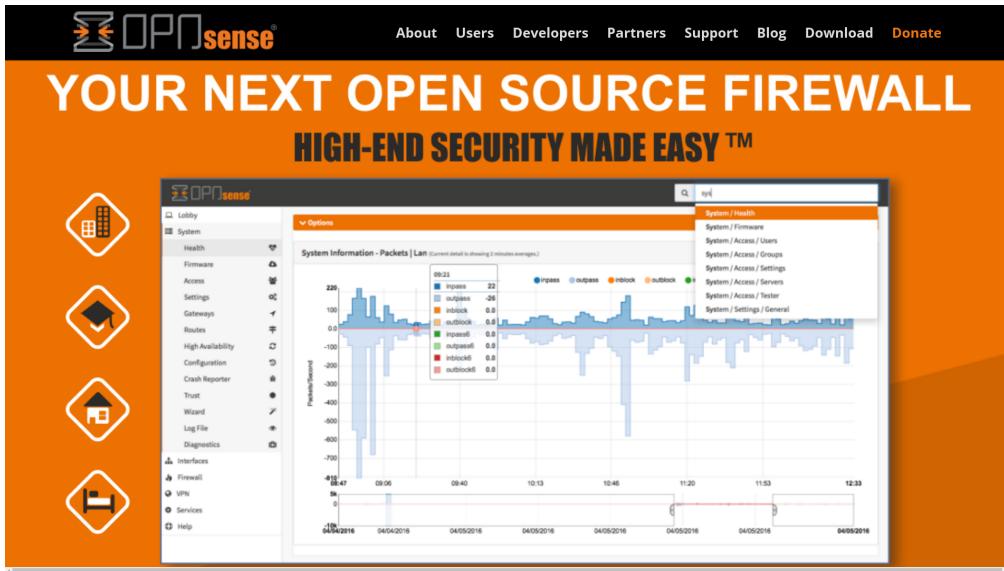


Figure 4.7: OPNsense Website

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

Can be tuned in.

4.5. OTHER

The screenshot shows the official OpenBSD website. On the left, there's a sidebar with links for "About OpenBSD", "Getting OpenBSD", "Getting Source", "OpenBSD Resources", and "Supporting OpenBSD". The main content area features a large "OPENBSD 5.9" logo with a cartoon illustration of a fish wearing a hat and scarf. Text above the logo reads "Free, functional, and secure". Below the logo, a sub-headline says "Only two remote holes in the default install, in a heck of a long time!". A paragraph explains the project's goals: "The OpenBSD project produces a **FREE**, multi-platform 4.4BSD-based UNIX-like operating system. Our efforts emphasize portability, standardization, correctness, [proactive security](#) and [integrated cryptography](#). As an example of the effort OpenBSD has, the popular [OpenSSH](#) software comes from OpenBSD." Another paragraph notes the availability: "OpenBSD is freely available from our download sites, or as a 3-CD set sold at [openbsdstore.com](#)". It also mentions the current release: "The current release is [OpenBSD 5.9](#), released March 29, 2016." Pre-orders for the next release are mentioned: "Pre-orders for the upcoming [OpenBSD 6.0](#) release are enabled at [openbsdstore.com](#)". Finally, it highlights community support: "OpenBSD is developed entirely by volunteers. The project's development environment and [developer events](#) are funded through contributions collected by [The OpenBSD Foundation](#). Contributions ensure that OpenBSD will remain a vibrant and [free](#) operating system."

Figure 4.8: OpenBSD Website

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
