



**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.

20160903

Contents

Introduction	
Aleph Objects Network	ix
1 pfSense	
Firewall.	11
1.1 Overview	12
1.2 Initial Configuration Overview	12
1.2.1 Setup via Serial Connection	13
1.2.2 Initial Wizard Setup via Web Browser	14
1.2.3 Basic Setup via Web Browser	14
1.2.4 SSL Certificate Manager Setup	15
1.2.5 General Setup	16
1.2.6 Initial Firewall Rules	16
1.2.7 Initial DNS Resolver Setup	16
1.2.8 Initial Logging Setup	17
1.2.9 Backup	17
1.2.10 Internet Connection	17
1.2.11 Update & Install Packages	18
1.2.12 OpenVPN	18
1.2.13 Turn off Internet via LAN	19
1.2.14 More Backup	20
1.3 NAT	20
1.4 Traffic Shaping	20
1.5 pfBlockerNG	20
1.6 Suricata	20
1.7 DHCP	21
1.8 NTP	22
1.9 OpenVPN	22
1.10 Captive Portal	23

CONTENTS

1.11 SSL Certificates	23
1.12 ssh	24
1.13 DNS	24
1.14 Routing	24
1.15 Interfaces	25
1.16 CARP and Synchronization	25
1.17 Reporting	25
2 iptables	
Stop.	27
2.1 Overview	28
2.2 iptables	28
3 Hardware	
Purchase Order	29
3.1 Overview	30
4 Switches	
Here.	31
4.1 Overview	32
4.2 Free Software for Network Switches	32
4.2.1 ONIE	32
4.2.2 Open Network Linux	33
4.2.3 Snaproute	34
4.2.4 OpenSwitch	35
4.2.5 FBOSS	36
4.2.6 Open Compute Project	38
4.2.7 OpenDataPlane	38
4.2.8 OpenFastPath	39
4.2.9 Open vSwitch	40
4.2.10 Big Switch	41
4.2.11 Uncategorized Software	41
4.3 Hardware	42
4.3.1 Edge-Core	42
4.3.2 Dell	42
4.3.3 Netberg	43
4.3.4 Quanta	43
4.3.5 Mellanox	44
4.4 Suppliers	45

CONTENTS

4.4.1	White Box	45
4.4.2	Bare Metal Switches	46
4.4.3	Colfax Direct	48
4.4.4	Penguin Computing	48
5	OS	
	Free Operating Systems	51
5.1	Requirements	52
5.2	Firewall Operating Systems in Use	53
5.2.1	Debian	53
5.2.2	pfSense	53
5.2.3	FreeBSD	55
5.3	Firewalls Evaluated	55
5.3.1	pfSense	55
5.3.2	Alpine Linux	56
5.3.3	clearOS	57
5.3.4	IPCop	60
5.3.5	IPFire	60
5.3.6	OPNsense	62
5.4	Previous Operating Systems in Use	63
5.4.1	OpenBSD	63
5.5	Other	64
5.5.1	Gentoo	64
5.5.2	NetBSD	64
6	Contact	
	Phone, Email, Web, Location	65
6.1	Support	66
6.2	Sales	66
6.3	Website	66

List of Figures

1.1	pfSense Website	12
1.2	Suricata Website	21
1.3	OpenVPN Website	22
1.4	Dnsmasq Website	24
1.5	ntopng Website	25
2.1	Netfilter Website	28
4.1	ONIE Website	32
4.2	Open Network Linux Website	34
4.3	Snaproute Website	35
4.4	OpenSwitch Website	36
4.5	FBOSS Website	37
4.6	OpenCompute Website	37
4.7	OpenDataPlane Website	38
4.8	OpenFastPath Website	39
4.9	Open vSwitch Website	40
4.10	Big Switch Website, no	41
4.11	Edge-core Website	42
4.12	Netberg Website	43
4.13	Quanta Website	44
4.14	Mellanox Website	44
4.15	Whitebox Website	45
4.16	Bare Metal Switches Website	46
4.17	Colfax Direct Website	49
5.1	Debian Website	54
5.2	FreeBSD Website	55
5.3	Alpine Linux Website	57
5.4	clearOS Website	58
5.5	IPCop Website	60
5.6	IPFire Website	61
5.7	OPNsense Website	62
5.8	OpenBSD Website	63

List of Listings

Introduction

Aleph Objects Network

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.

pfSense

Firewall.

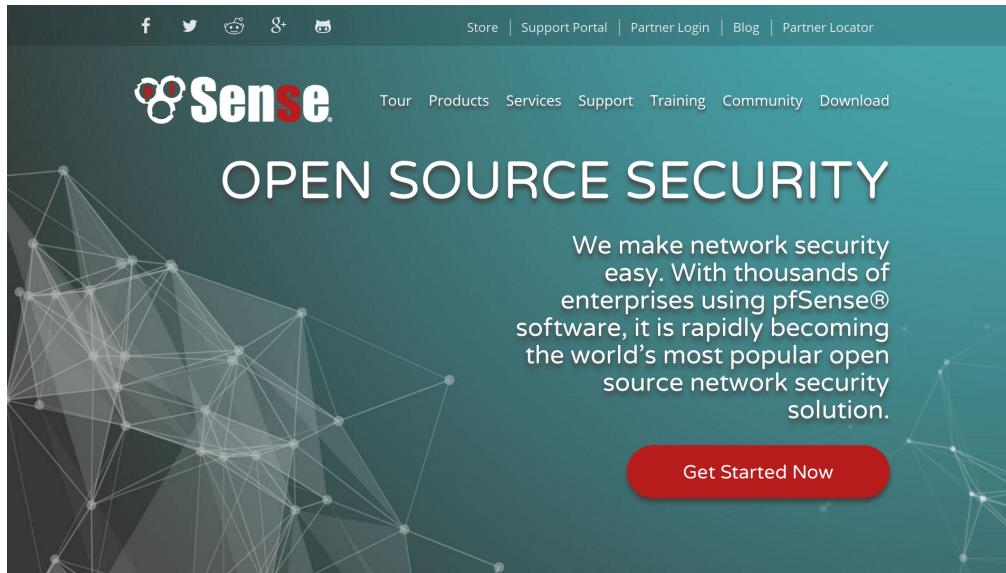


Figure 1.1: pfSense Website

1.1 Overview

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

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 Overview

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 to pfSense firewall via web browser.

1.2. INITIAL CONFIGURATION OVERVIEW

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 via Serial Connection

1. Plug the pfSense provided USB cable into the Console port on the firewall and the USB port of your Debian workstation.
2. 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
```

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

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

4. 115200 baud, 8N1, no flow control.
5. Copy MAC address to main DHCP/DNS server, and reserve IP address.
6. Set IP for LAN (e.g. 192.168.1.1)
7. Set IP for WAN, disable IPv6

1.2.2 Initial Wizard Setup via Web Browser

1. Log in to firewall (e.g. <https://192.168.1.1>). Initial pass admin/pfsense.
2. Start Wizard, hit Next.
3. pfSense Gold, Next.
4. Hostname: set hostname.
5. Set WAN, LAN, password, etc.
6. Hit Reload, and the wizard is done.

1.2.3 Basic Setup via Web Browser

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

1.2. INITIAL CONFIGURATION OVERVIEW

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.

1.2.4 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.

1.2.5 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 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.

1.2.6 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.

1.2.7 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. INITIAL CONFIGURATION OVERVIEW

1.2.8 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.

1.2.9 Backup

Make first backup.

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

1.2.10 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 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..

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.

1.2.11 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.

1.2.12 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
```

1.2. INITIAL CONFIGURATION OVERVIEW

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 internal 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).

1.2.13 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.

1.2.14 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.

- barnyard2

1.7. DHCP

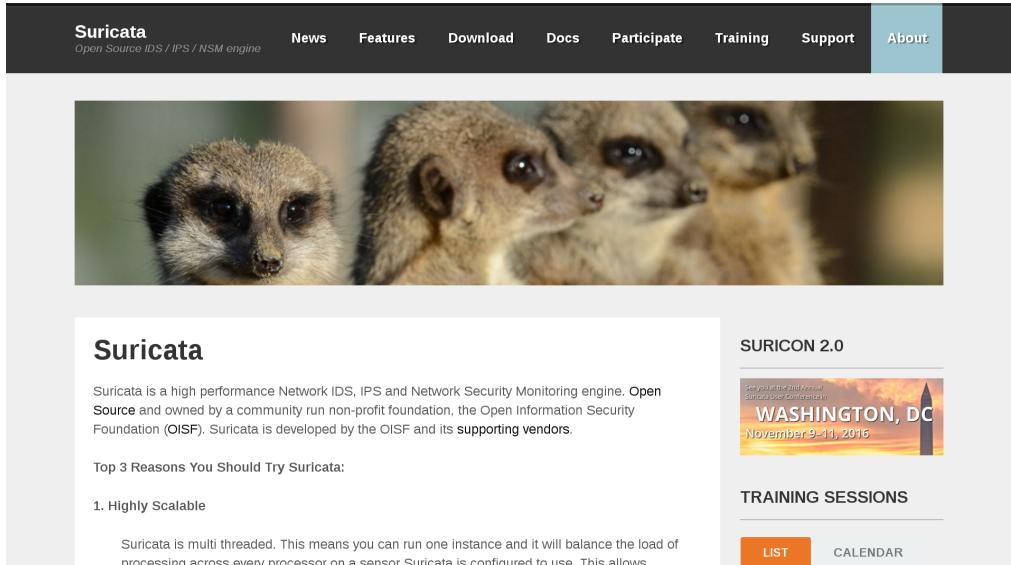


Figure 1.2: Suricata Website

- 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/pixelinux.0 or jessie/pixelinux.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



Figure 1.3: OpenVPN Website

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.”

1.10. CAPTIVE PORTAL

- 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.
- 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.



Dnsmasq provides network infrastructure for small networks: DNS, DHCP, router advertisement and network boot. It is designed to be lightweight and have a small footprint, suitable for resource constrained routers and firewalls. It has also been widely used for tethering on smartphones and portable hotspots, and to support virtual networking in virtualisation frameworks. Supported platforms include Linux (with glibc and uclibc), Android, *BSD, and Mac OS X. Dnsmasq is included in most Linux distributions and the ports systems of FreeBSD, OpenBSD and NetBSD. Dnsmasq provides full IPv6 support.

The DNS subsystem provides a local DNS server for the network, with forwarding of all query types to upstream recursive DNS servers and cacheing of common record types (A, AAAA, CNAME and PTR, also DNSKEY and DS when DNSSEC is enabled).

- Local DNS names can be defined by reading /etc/hosts, by importing names from the DHCP subsystem, or by configuration of a wide range of useful record types.
- Upstream servers can be configured in a variety of convenient ways, including dynamic configuration as these change on moving upstream network.
- Authoritative DNS mode allows local DNS names may be exported to zone in the global DNS. Dnsmasq acts as authoritative server for this zone, and also provides zone transfer to secondaries for the zone, if required.
- DNSSEC validation may be performed on DNS replies from upstream nameservers, providing security against spoofing and cache poisoning.
- Specified sub-domains can be directed to their own upstream DNS servers, making VPN configuration easy.

Figure 1.4: Dnsmasq Website

1.14 Routing

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

1.15 Interfaces

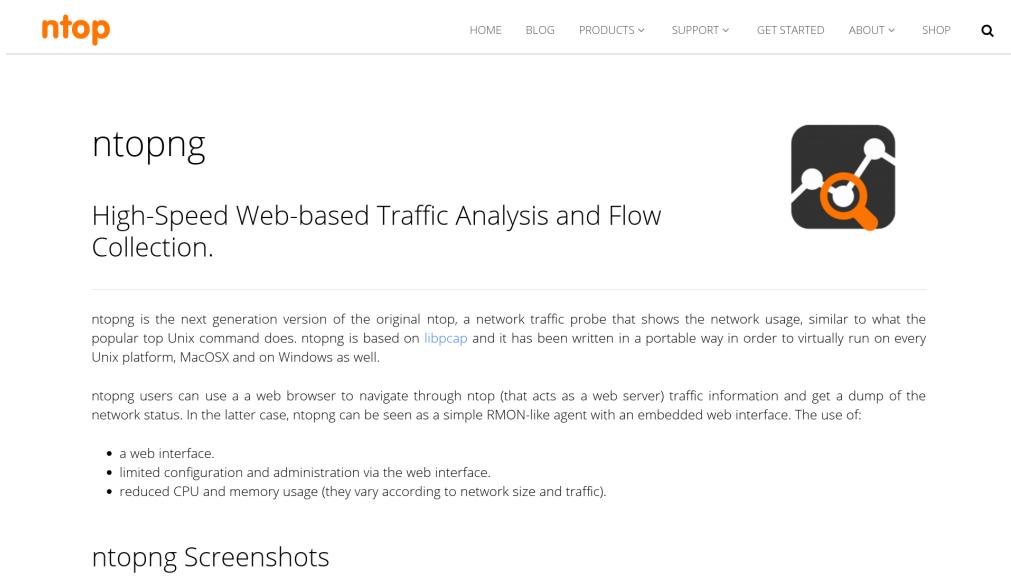
- Gigabit ethernet.
- SFP+.
- Hardware offloading (e.g. checksums).

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



The screenshot shows the ntopng website. At the top, there is a navigation bar with links for HOME, BLOG, PRODUCTS, SUPPORT, GET STARTED, ABOUT, and SHOP, along with a search icon. Below the navigation bar, the word "ntop" is displayed in orange. The main content area features the title "ntopng" in large orange text, followed by a subtitle "High-Speed Web-based Traffic Analysis and Flow Collection." To the right of the subtitle is a graphic icon depicting a magnifying glass over a network of nodes connected by lines. A horizontal line separates this from the descriptive text below. The text explains that ntopng is the next generation version of the original ntop, a network traffic probe, and provides a link to libpcap. It also notes that ntopng is portable and runs on various platforms. Further down, it describes the use of ntopng for web-based traffic analysis and flow collection, mentioning its use as a web server and RMON-like agent. A final section titled "ntopng Screenshots" is shown at the bottom.

Figure 1.5: ntopng Website

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

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

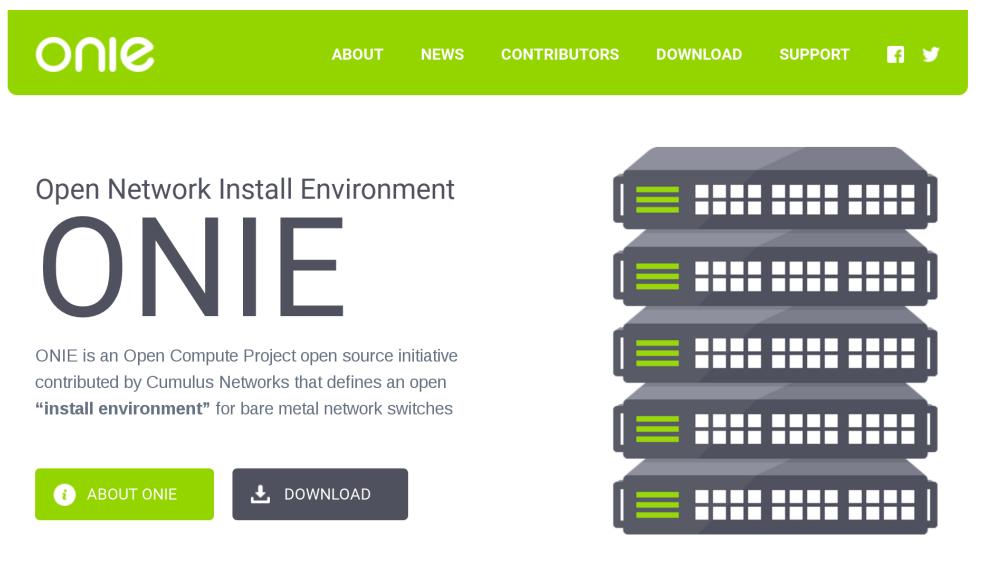


Figure 4.1: ONIE Website

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

4.2. 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.”

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

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 is a large white area containing text and an image. On the left, the text describes Open Network Linux as a "bare metal" Linux distribution for network forwarding devices built from commodity components. It mentions the use of ONIE for installation onto on-board flash memory and its role in the Open Compute Project. On the right, there is an illustration of a black and white penguin sitting on top of a grey server rack with multiple ports.

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.

4.2. FREE SOFTWARE FOR NETWORK SWITCHES

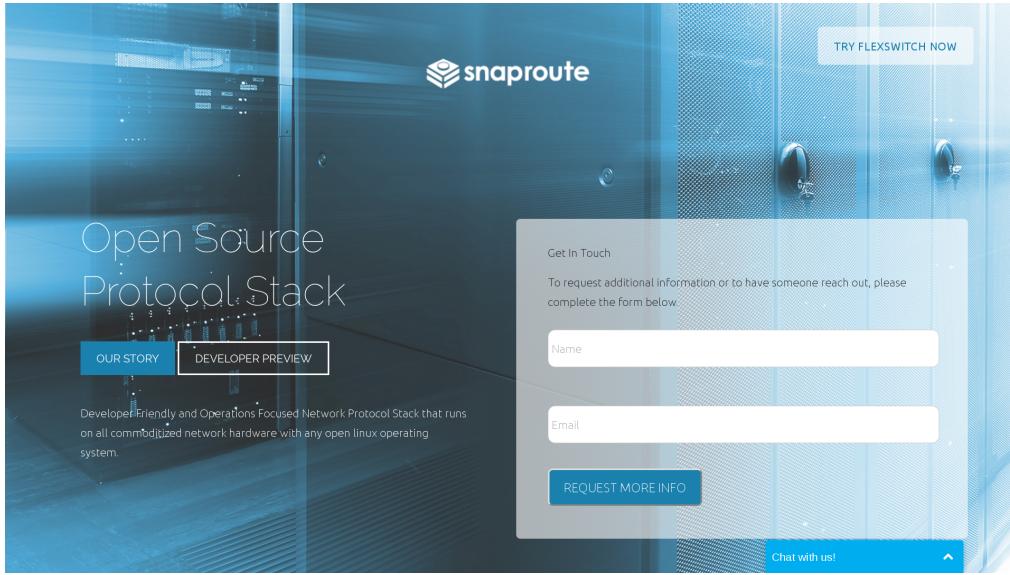


Figure 4.3: Snaproute Website

- 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 compatibility 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.

4.2. 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 commits, 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 4.5: FBOSS Website

The screenshot shows the OpenCompute Project 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 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

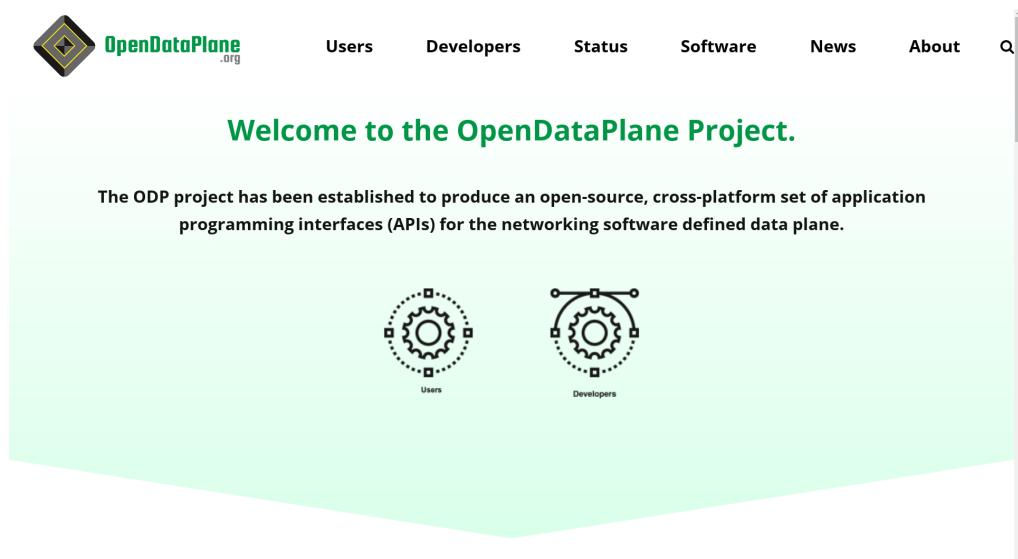


Figure 4.7: OpenDataPlane Website

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

4.2. 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/>

4.2.8 OpenFastPath

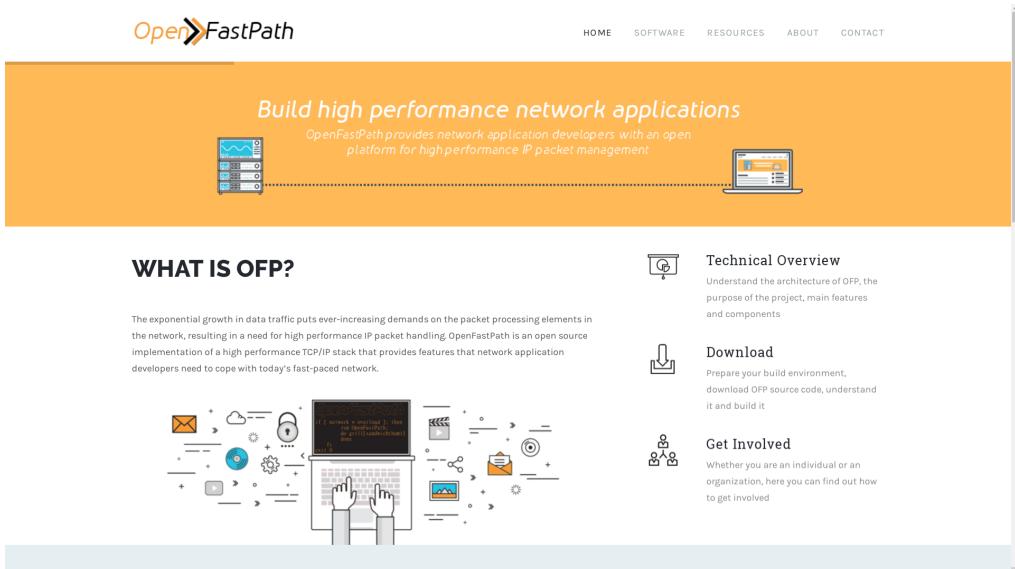


Figure 4.8: OpenFastPath Website

- 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

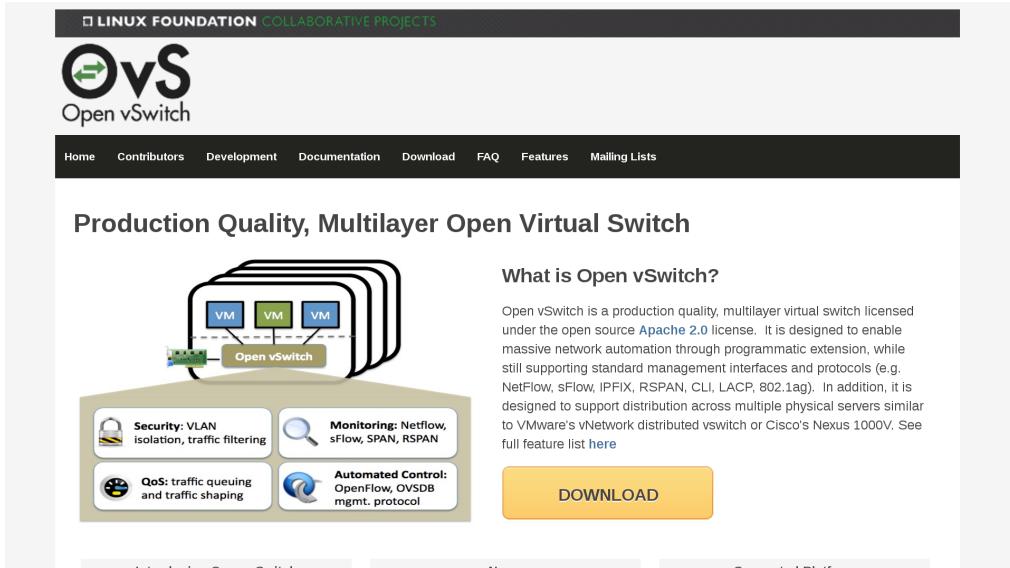


Figure 4.9: Open vSwitch Website

- 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. FREE SOFTWARE FOR NETWORK SWITCHES

4.2.10 Big Switch



Figure 4.10: 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.

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

Switches

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

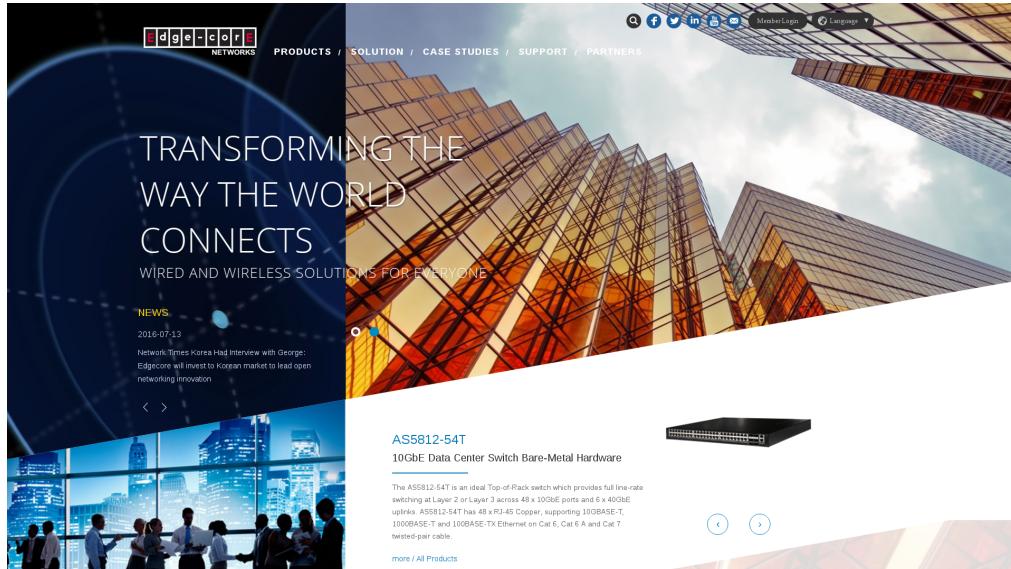


Figure 4.11: Edge-core Website

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

4.3.2 Dell

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

4.3. HARDWARE

Dell makes some bare metal switches that are ONIE compatible.

4.3.3 Netberg

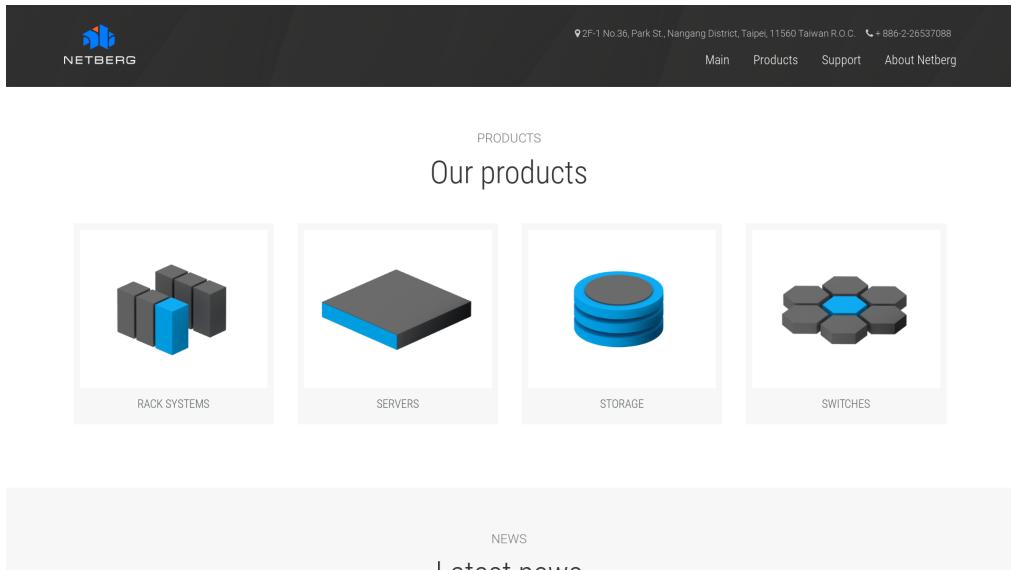


Figure 4.12: Netberg Website

- 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.

Switches



FROM HYPERSCALE TO HYPER CONVERGED

Figure 4.13: Quanta Website

4.3.5 Mellanox



Figure 4.14: Mellanox Website

4.4. SUPPLIERS

- 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

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.

4.4.2 Bare Metal Switches

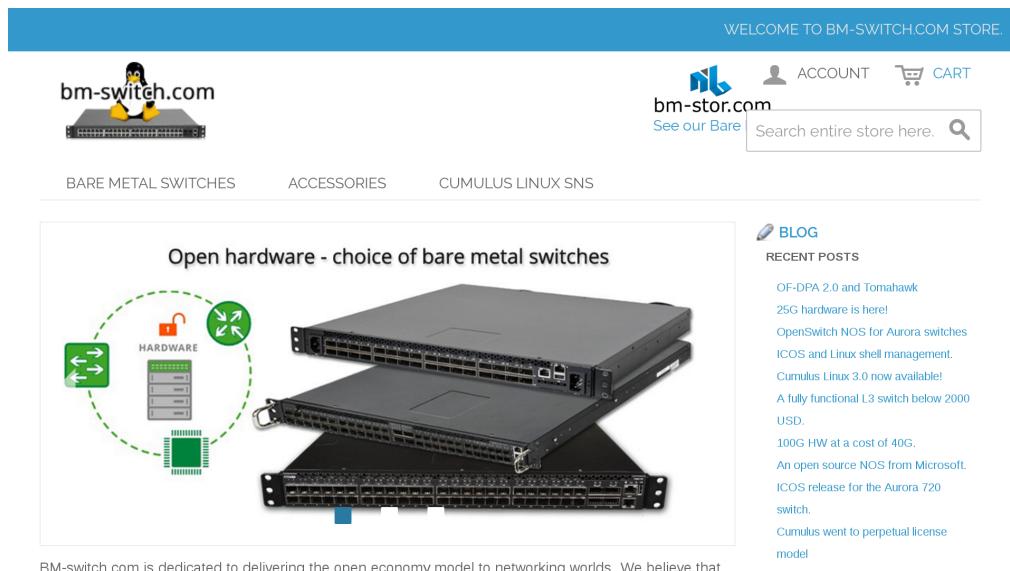


Figure 4.16: Bare Metal Switches Website

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

4.4. 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

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/>

4.4. 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, navigation links 1, 2, 3, 4, 5.
- Bottom Content:** Adapters section with three 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 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?).

5.2. 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

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.

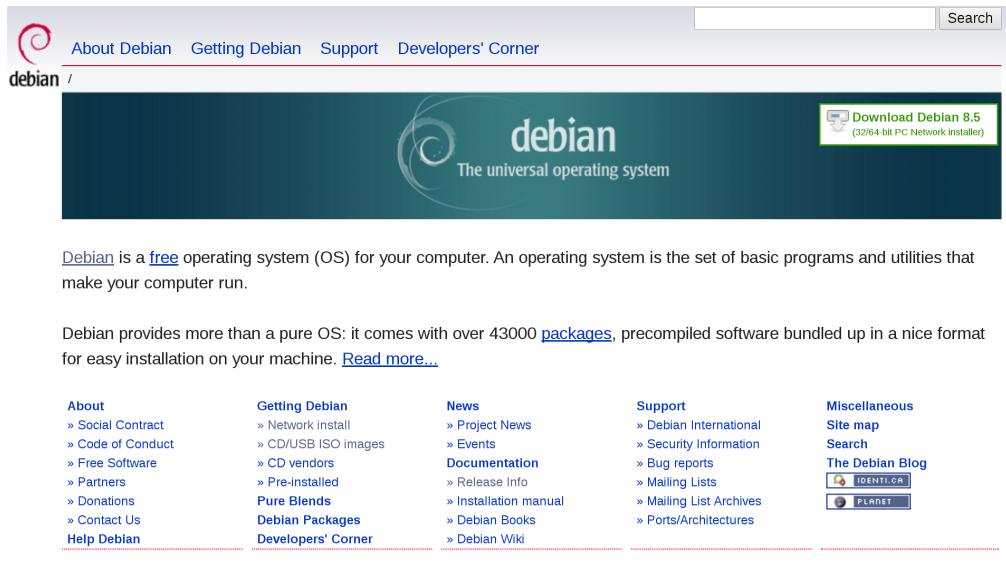


Figure 5.1: Debian Website

- 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 ...

5.3. FIREWALLS EVALUATED

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.

5.3. FIREWALLS EVALUATED

The screenshot shows the official Alpine Linux website. At the top, there's a navigation bar with links for 'home', 'downloads', 'about', 'community', and 'sponsors'. Below the navigation bar, there's a search bar and a link to 'Wiki'. The main content area features a large download button for 'alpine-3.4.3-x86_64.iso' (83MB), which was released on 2016-08-23. To the left of the download button, there's a section titled 'Small. Simple. Secure.' with a brief description of Alpine Linux. On the right side of the main content area, there are two sections: 'Alpine News' and 'Latest Development', each listing recent releases and changes.

Small. Simple. Secure.

Alpine Linux is a security-oriented, lightweight Linux distribution based on musl libc and busybox.

Alpine News

2016-08-12 Alpine 3.4.3 released
2016-07-25 Alpine 3.4.2 released
2016-06-28 Alpine 3.4.1 released
2016-05-31 Alpine 3.4.0 released
2016-03-24 Alpine 3.3.3 released
2016-03-18 Alpine 3.3.2 released
2016-01-06 Alpine 3.3.1 released
2016-01-06 Alpine 3.3.0 released

Latest Development

2016-08-23 community/crackmapexec: moved from testing, uses specific python2 packages
2016-08-23 community/py-gevent: moved from testing, upgraded to 1.1.2, added python3 support and py2/py3 subpackages
2016-08-23 community/py-greenlet: moved from testing, added python3 support, added py2/py3 subpackages
2016-08-23 community/nut-terminal: moved from testing

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

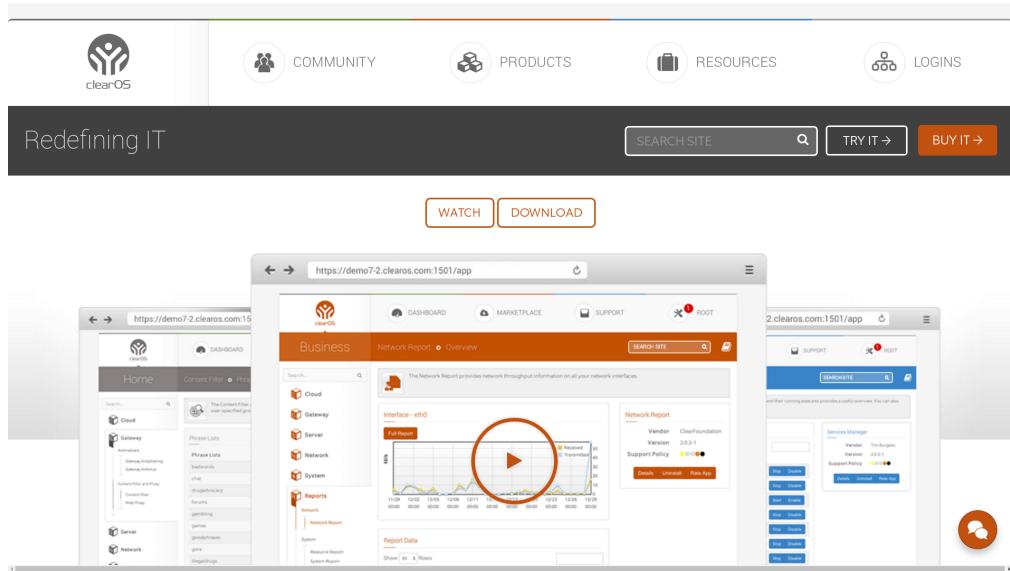


Figure 5.4: clearOS Website

- 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).

5.3. FIREWALLS EVALUATED

- 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.

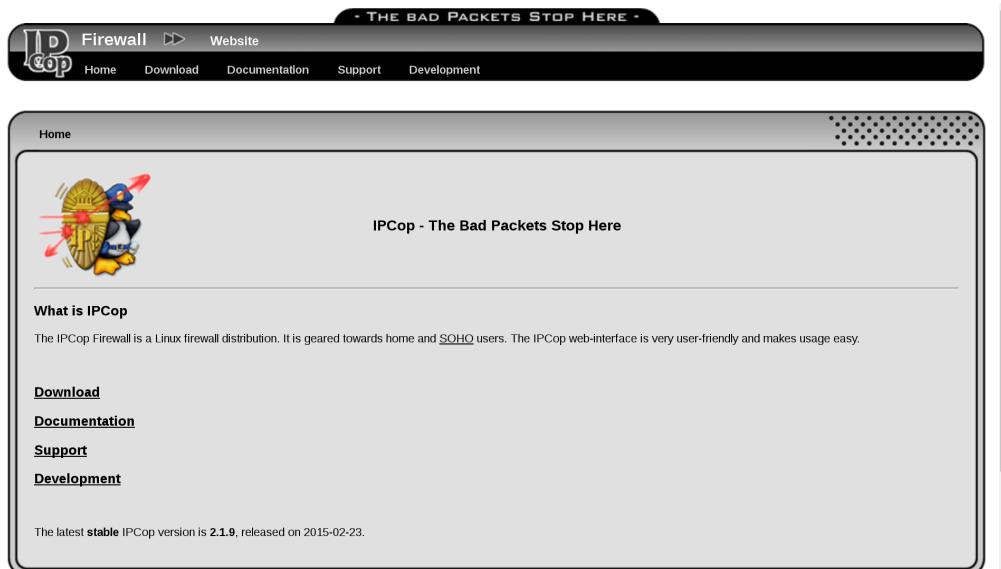


Figure 5.5: IPCop Website

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 crusty 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

5.3. FIREWALLS EVALUATED

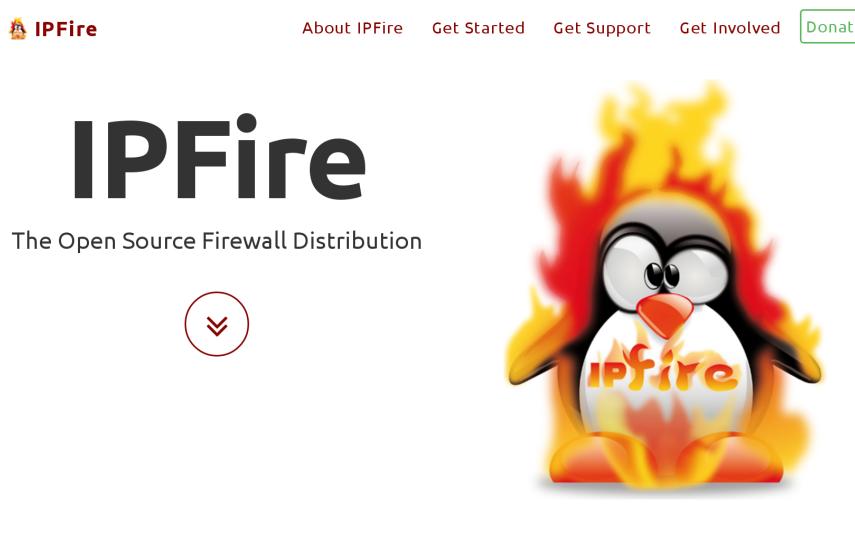


Figure 5.6: IPFire Website

- 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”

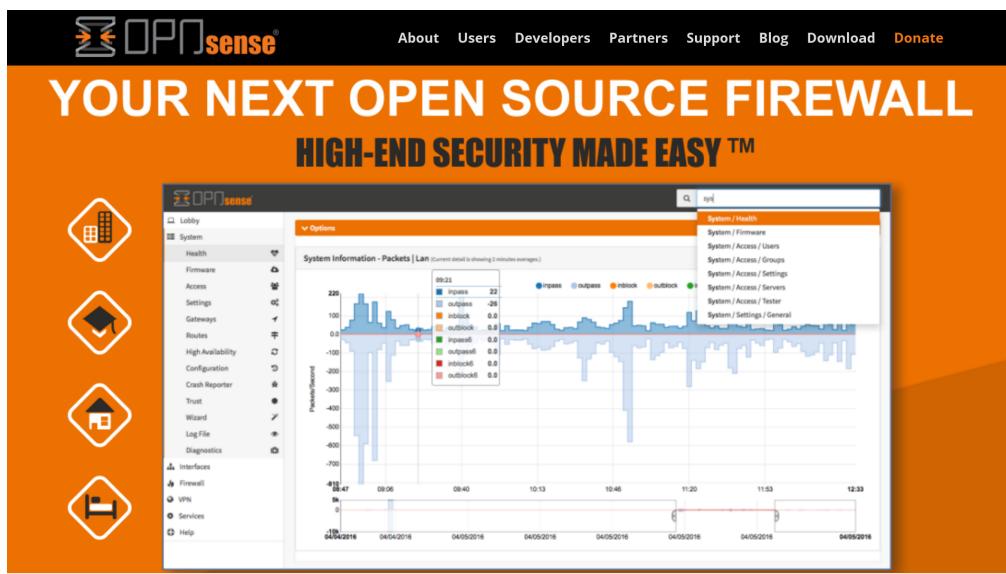


Figure 5.7: OPNsense Website

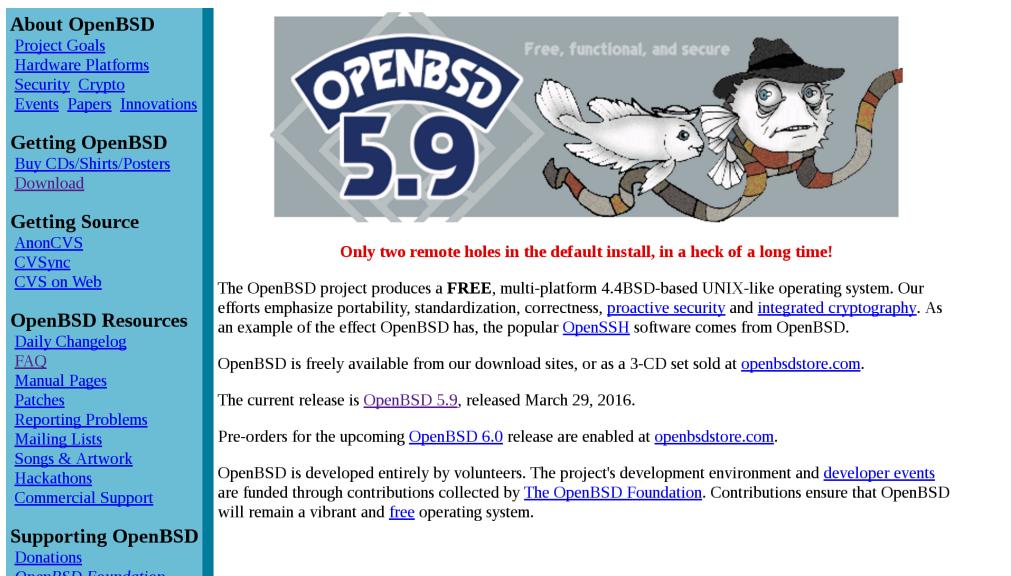
- Release is current.
- Making a dd of the .iso to a USB drive didn't boot. OPNsense-16.7.r2-OpenSSL-cdrom-amd64.iso

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

5.4 Previous Operating Systems in Use

5.4.1 OpenBSD

OpenBSD



The screenshot shows the official OpenBSD website. On the left, there's a vertical navigation bar with sections like 'About OpenBSD', 'Getting OpenBSD', 'Getting Source', 'OpenBSD Resources', and 'Supporting OpenBSD'. The main content area features a large banner for 'OPENBSD 5.9' with the tagline 'Free, functional, and secure'. Below the banner is a cartoon illustration of a fish-like character wearing a top hat and a scarf, carrying a briefcase. A caption below the illustration reads 'Only two remote holes in the default install, in a heck of a long time!'. The text explains that OpenBSD produces a FREE, multi-platform 4.4BSD-based UNIX-like operating system, emphasizing portability, standardization, correctness, proactive security, and integrated cryptography. It mentions the popularity of OpenSSH and the availability of the software from download sites or a 3-CD set. The current release is OpenBSD 5.9, released March 29, 2016. Pre-orders for OpenBSD 6.0 are available at openbsdstore.com. The page also notes that OpenBSD is developed entirely by volunteers, with contributions from The OpenBSD Foundation ensuring its vibrancy and freedom.

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
