ALEPH OBJECTS®
INCORPORATED

FIREWALL

Aleph Objects Firewall

by Aleph Objects, Inc.

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

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

20160825

Contents

List of Figures

Introduction

Firewall

Aleph Objects' HQ uses an OpenBSD router to connect to the Internet. We would like to upgrade it, using the best free software solutions.

Firewall

Stop.

1.1 Overview

Firewall.

- Must be free software.
- The project must still be alive.
- Does it use a hardened kernel?
- How does it do security updates?
- Are there open security issues?
- Are there any CVEs?
- How are security issues handled?
- Is there a list of security issues?
- Does it have a wifi portal? (Should that be a separate box or in OpenWRT?)
- Does upstream https actually work?
- UTM - Unified Threat Management (e.g. snort, etc.)
- Load balancing between multiple upstreams (without BGP).
- Load balancing between dual local routers.
- Fail over to standby router (e.g. pfsync).
- "Anti-virus", SMTP, POP scans? Meh? (e.g. OpenBSD has greylist/tarpit.)
- Packet cleansing (e.g. tcp header randomization).
- Do we want DNS, DHCP, etc? Probably not?
- OpenVPN (built into router, or thru it?).
- Network graphing (MRTG, aguri, etc.)
- No broken "community" editions.

- Have mirrored server doing analysis?
- NAT options? cone, etc.
- Local system monitoring (e.g. system temp, hdd status, etc.)
- sshd
- GSM, pppd ?
- Two-factor authentication.
- snort, suricata

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 now many new free software solutions for network switches. Unfortunately, they are all high-end data center gear, the least expensive costing over $3,000USD.

3.2 Open Compute Project

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

Project so massive data centers can be more "open" and interoperate better between vendors, by using free software.

3.3 ONIE

onie.org Open Network Install Environment. Used to install an OS to a switch. Comes pre-installed from switch manufacturer.

3.4 Open Network Linux

opennetlinux.org Distro for bare metal switches.

- BIRD – http://bird.network.cz/
- Quagga – http://www.quagga.net/
- OpenNSL – Broadcom chipsets. Accton. Github archive has proprietary license (LICENSE-Adv = non-free).
- OF-DPA – From Broadcom.
- SAI
- FBOSS
- Azure SONiC
- FlexSwitch – OpenSnaproute – Snaproute

OS

Free Operating Systems

There are a lot of operating systems to consider...

4.1 Debian

Debian

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

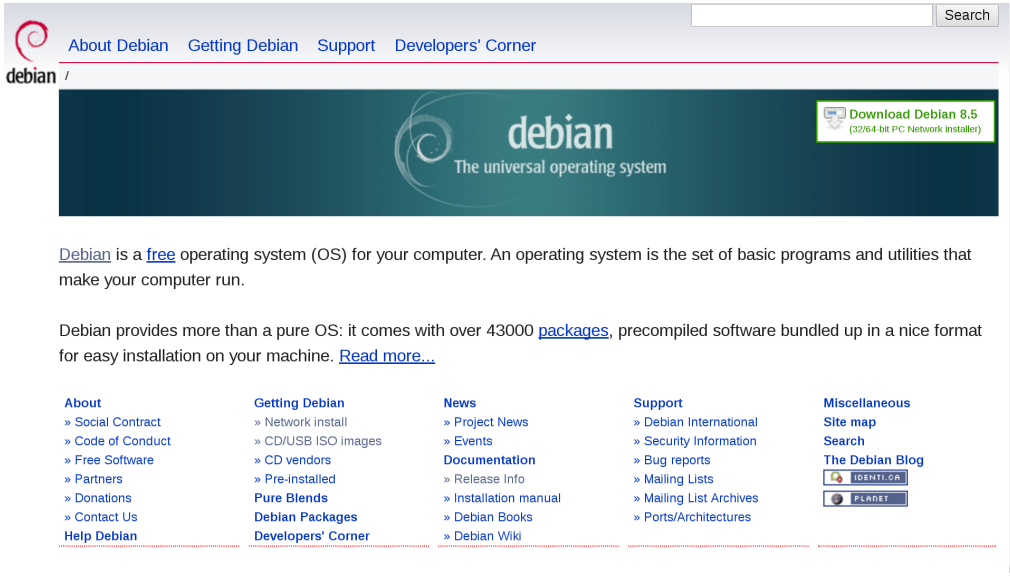

Figure 4.1: Debian Website

4.2 OpenBSD

OpenBSD

We are using OpenBSD right now for our firewall. It is very reliable and secure. Few people know how to administer it. It is all command line editing of firewall configuration files. We are potentially switching away from it to get something easier to use and that has more analytics.

4.3 Gentoo

Gentoo
Can be tuned in.

4.4 FreeBSD

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

4.5 NetBSD

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

4.6 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.

4.7 clearOS

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

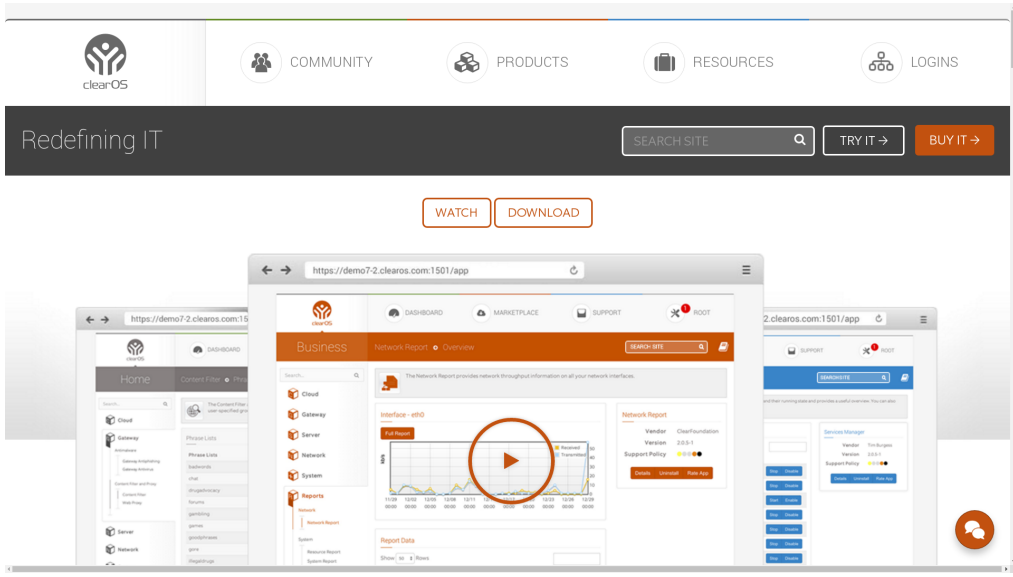

Figure 4.2: clearOS Website

- Overall, very very nice, very clean with many features.
- Baitware is the only thing holding this back.
- The web interface never crashed or caused issues.
- Usage is stable.
- Latest release: 7.2.0
- Release Date: March 7, 2015.
- Package Updater: yum
- Kernel: Linux 3.10.0-327.3.1.el17.x86_64
- Base OS: Fedora? CentOS?
- Easy GUI install
- Has enterprise (baitware?) version.
- Has enterprise hardware.

- Web based configuration system started on first boot
- Web wizard has option to select Community or non-free versions.
- Web wizard has system registration for a marketplace for apps. Have to register?
- Registering set "Software End-of-Life" to August 31, 2018.
- Lots of phone-home activity with marketplace and registration....
- Simple "Update All" button to update system (with yum, afaict).
- Very clean, overall.
- Wide variety of "Apps" in the Marketplace that are GPL.
- Non-free plugins are listed along free ones. The owncloud plugin is non-free.
- Most apps don't have any ratings,
- The default "Exception Sites" whitelist had their clear*.com sites and a few *.microsoft.com.
- Has optionally transparent web proxy.
- Installed many Apps, and it was all very clean.
- clearOS gets pwned, we get pwnd? Yes.
- Need to create account to get to knowledge base ?
- Actual firewalling rules (e.g. block just these devices from everything but port 443) aren't so strong.
- There doesn't appear to be a way to say "just allow port 22 from NNN"...
- A lot of great setup.
- MultiWAN — Nice, but simple load balancing between multiple upstreams.

- Failover to multiple upstreams.
- No fail over to another router (ala CARP).
- dhclient (?) overwrites DNS addresses, no place to set static (?!?)
- Some pretty graphs, but not the most useful.

4.8 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."

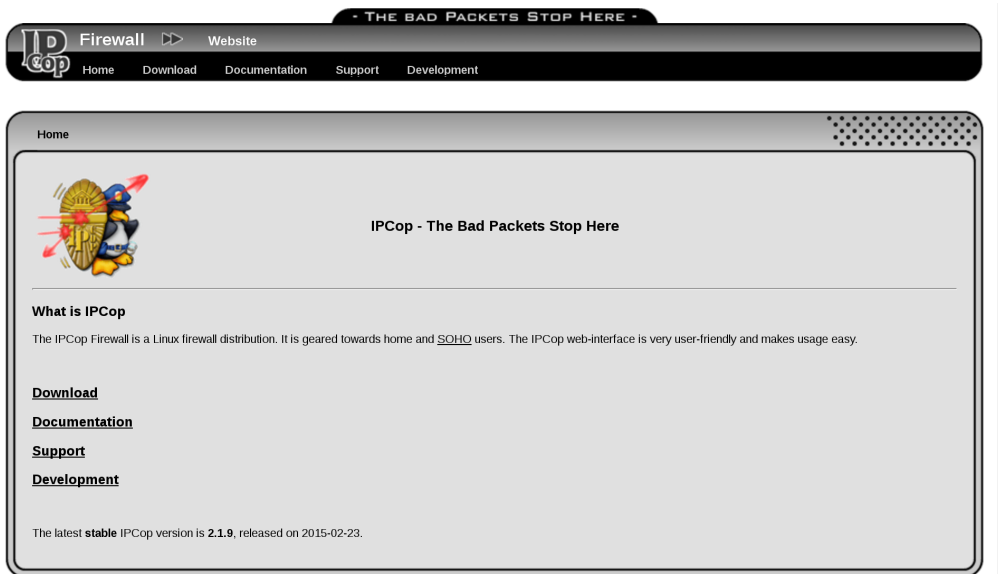

Figure 4.3: IPCop Website

- 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 crufty at this point.

4.9 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 4.4: 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 (?).

- 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 (!).

4.10 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

4.11 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."

Figure 4.5: OPNsense Website

Figure 4.6: pfSense Website

- 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 ...

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