



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.

20160707

Contents

Introduction	
Firewall	vii
1 Firewall	
Stop.	9
1.1 Overview	10
2 Authentication	
Who?	13
2.1 Overview	14
3 Routers	
There.	15
3.1 Overview	16
4 Analytics	
Wha?	17
4.1 Overview	18
5 Hardware	
Purchase Order	19
5.1 Overview	20
6 Switches	
Here.	21
6.1 Overview	22
6.2 Open Compute Project	22
6.3 ONIE	22
6.4 Open Network Linux	22
7 NOS	
Network Operating System	23

CONTENTS

7.1	Overview	24
8	Contact	
	Phone, Email, Web, Location	25
8.1	Support	26
8.2	Sales	26
8.3	Website	26

List of Figures

Introduction

Firewall

Introduction

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?)
- 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?

1.1. OVERVIEW

- NAT options? cone, etc.
- Local system monitoring (e.g. system temp, hdd status, etc.)
- sshd
- GSM, pppd ?
- Two-factor authentication.

Authentication

Who?

2.1 Overview

Two-factor authentication using TOTP.

Routers

There.

3.1 Overview

Routers.

Analytics

Wha?

4.1 Overview

What is the network doing?

- snort
- MRTG
- Aguri

Hardware Purchase Order

5.1 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.

6.1 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.

6.2 Open Compute Project

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

6.3 ONIE

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

6.4 Open Network Linux

opennetlinux.org Distro for bare metal switches.

NOS

Network Operating System

7.1 Overview

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

- Debian
- OpenBSD
- Gentoo
- FreeBSD
- NetBSD
- alpine
- clearos
- ipcop
- ipfire
- opnsense
- pfsense
- zentyal

Contact

Phone, Email, Web, Location

8.1 Support

Email: support@alephobjects.com

Phone: +1-970-377-1111 x610

8.2 Sales

Email: sales@alephobjects.com

Phone: +1-970-377-1111 x600

8.3 Website

Aleph Objects, Inc.

www.alephobjects.com

Colophon

Created with 100% Free Software
Debian GNU/Linux
L^AT_EX Memoir
