



**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.

20160905

Contents

Introduction	
Aleph Objects Network	ix
1 pfSense	
Firewall.	11
1.1 Overview	12
1.2 Initial Configuration	12
1.2.1 Setup pfSense Hardware	13
1.2.2 Setup via Serial Connection	14
1.2.3 Initial Wizard Setup via Web Browser	19
1.2.4 Initial Dashboard	25
1.2.5 Moar Configuration	26
1.2.6 Set Up a New User	27
1.2.7 SSH Access	29
1.2.8 Admin Access Configuration	29
1.2.9 Advanced Networking Configuration	31
1.2.10 Advanced Miscellaneous Configuration	32
1.2.11 Advanced Notifications Configuration	33
1.2.12 SSL Create a Certificate Signing Request	34
1.2.13 SSL Retrieve and Submit a Certificate Signing Request	35
1.2.14 SSL Install New Certificate	36
1.2.15 SSL Import Gandi Certificate Authority	36
1.2.16 SSL Certificate Revocations	37
1.2.17 General Setup	37
1.2.18 Use New SSL Certificate for Web Admin	37
1.2.19 Initial Firewall Rules	38
1.2.20 Initial DNS Resolver Setup	38
1.2.21 Dynamic DNS Setup	39
1.2.22 Initial Logging Setup	39

CONTENTS

1.2.23 Initial Dashboard Setup	40
1.2.24 Backup	40
1.2.25 Reboot	40
1.2.26 Internet Connection	41
1.2.27 Update & Install Packages	41
1.2.28 Set Up sudo User	42
1.2.29 OpenVPN Certificates	42
1.2.30 OpenVPN Setup	43
1.2.31 OpenVPN User Certificate Creation	44
1.2.32 OpenVPN User Certificate Export	45
1.2.33 Turn off Internet via LAN	45
1.2.34 Backup	46
1.2.35 Reboot	46
1.3 NAT	46
1.4 Traffic Shaping	46
1.5 pfBlockerNG	46
1.6 Suricata	47
1.7 DHCP	47
1.8 NTP	48
1.9 OpenVPN	48
1.10 Captive Portal	49
1.11 SSL Certificates	49
1.12 ssh	50
1.13 DNS	50
1.14 Routing	50
1.15 Interfaces	50
1.16 CARP and Synchronization	51
1.17 Reporting	51
2 iptables	
Stop.	53
2.1 Overview	54
2.2 iptables	54
3 Hardware	
Purchase Order	55
3.1 Overview	56

CONTENTS

4 Switches Here.		57
4.1 Overview		58
4.2 Free Software for Network Switches		58
4.2.1 ONIE		58
4.2.2 Open Network Linux		59
4.2.3 Snaproute		60
4.2.4 OpenSwitch		61
4.2.5 FBOSS		62
4.2.6 Open Compute Project		64
4.2.7 OpenDataPlane		64
4.2.8 OpenFastPath		65
4.2.9 Open vSwitch		66
4.2.10 Big Switch		67
4.2.11 Uncategorized Software		67
4.3 Hardware		68
4.3.1 Edge-Core		68
4.3.2 Dell		69
4.3.3 Netberg		69
4.3.4 Quanta		69
4.3.5 Mellanox		70
4.4 Suppliers		70
4.4.1 White Box		70
4.4.2 Bare Metal Switches		72
4.4.3 Colfax Direct		74
4.4.4 Penguin Computing		75
5 OS		
Free Operating Systems		77
5.1 Requirements		78
5.2 Firewall Operating Systems in Use		79
5.2.1 Debian		79
5.2.2 pfSense		79
5.2.3 FreeBSD		81
5.3 Firewalls Evaluated		81
5.3.1 pfSense		81
5.3.2 Alpine Linux		82
5.3.3 clearOS		83

CONTENTS

5.3.4	IPCop	86
5.3.5	IPFire	86
5.3.6	OPNsense	88
5.4	Previous Operating Systems in Use	89
5.4.1	OpenBSD	89
5.5	Other	90
5.5.1	Gentoo	90
5.5.2	NetBSD	90
6	Contact	
	Phone, Email, Web, Location	91
6.1	Support	92
6.2	Sales	92
6.3	Website	92

List of Figures

1.1	pfSense Website	12
1.2	pfSense Console Using <code>minicom</code>	14
1.3	pfSense <code>minicom</code> Settings	15
1.4	pfSense Cert Authority Invalid	20
1.5	pfSense Login	21
1.6	pfSense Wizard	21
1.7	pfSense Gold	22
1.8	pfSense Wizard General Information	22
1.9	pfSense Wizard Timezone	23
1.10	pfSense Wizard WAN Configuration	23
1.11	pfSense Wizard LAN Configuration	24
1.12	pfSense Wizard Admin Password	25
1.13	pfSense Wizard Reload Configuration	25
1.14	pfSense Wizard Reloading	26
1.15	pfSense Wizard Complete	26
1.16	pfSense Initial Dashboard	27
1.17	pfSense Menu: System, User Manager, Users	27
1.18	pfSense Menu: System, User Manager, Add User	28
1.19	pfSense Via SSH, Running <code>top</code>	29
1.20	pfSense Menu: System, Advanced, Admin Access	30
1.21	pfSense Menu: System, Advanced, Networking	32
1.22	pfSense Menu: System, Advanced, Miscellaneous	33
1.23	pfSense Menu: System, Advanced, Notifications	34
1.24	Suricata Website	47
1.25	OpenVPN Website	48
1.26	Dnsmasq Website	50
1.27	ntopng Website	51
2.1	Netfilter Website	54
4.1	ONIE Website	58
4.2	Open Network Linux Website	60
4.3	Snaproute Website	61
4.4	OpenSwitch Website	62

List of Figures

4.5	FBOSS Website	63
4.6	OpenCompute Website	63
4.7	OpenDataPlane Website	64
4.8	OpenFastPath Website	65
4.9	Open vSwitch Website	66
4.10	Big Switch Website, no	67
4.11	Edge-core Website	68
4.12	Netberg Website	69
4.13	Quanta Website	70
4.14	Mellanox Website	71
4.15	Whitebox Website	71
4.16	Bare Metal Switches Website	72
4.17	Colfax Direct Website	75
5.1	Debian Website	80
5.2	FreeBSD Website	81
5.3	Alpine Linux Website	83
5.4	clearOS Website	84
5.5	IPCop Website	86
5.6	IPFire Website	87
5.7	OPNsense Website	88
5.8	OpenBSD Website	89

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.

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

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 via ethernet to pfSense firewall with web browser.

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 pfSense Hardware

The following pfSense hardware has been tested:

- **SG-2220** — Two 1Gb ethernet ports, dual core 1.7GHz, 2GB RAM, 60GB SSD, single 100-240V power supply, fanless.
- **SG-2440** — Four 1Gb ethernet ports, dual core 1.7GHz, 4GB RAM, 128GB SSD, single 100-240V power supply, fanless.
- **SG-4860** — Six 1Gb ethernet ports, quad core 2.4GHz, 8GB RAM, 128GB SSD, single 100-240V power supply, fanless.
- **XG-2758** — High availability, ten 1Gb ethernet, two 10Gb SFP+ modules, eight core 2.4GHz, 16GB RAM 120GB RAID SSD, single 90-264V power supply, fans, 1U rackmount.

Follow these steps to get the hardware set up to configure the pfSense router.

1. Leave the power off for now.
2. Leave the WAN port unplugged for now.
3. Plug the pfSense provided USB cable into the Console port on the firewall and the USB port of your Debian workstation.
4. Plug in the LAN ethernet port into the local LAN switch.

```

Starting DHCP service...done.
Starting DHCPv6 service...done.
Configuring firewall.....done.
Generating RRD graphs...done.
Starting watchdog daemon...iCHWD0 on isa0
pcibus0: Cannot reserve I/O port range
done.
Starting syslogd...done.
Starting cron...done.
Starting package AutoconfigBackup...done.
Starting package AWS VPC Wizard...done.
Starting package IPsec Profile Wizard...done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Wed Jul 20 10:29:55 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (tty1)
*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***
MAN (wan)    -> igb1      ->
LAN (lan)    -> igb0      -> v4: 192.168.1.1/24
OPT1 (opt1)  -> igb2      ->
OPT2 (opt2)  -> igb3      ->
OPT3 (opt3)  -> igb4      ->
OPT4 (opt4)  -> igb5      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Restore factory defaults   13) Reboot system
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: [CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyUSB0]

```

Figure 1.2: pfSense Console Using `minicom`

1.2.2 Setup via Serial Connection

With the hardware all plugged in, connect with `minicom` and do some initial configuration via the USB port. Note, it is possible to start configuration by going to <https://192.168.1.1> if you set an IP address on your Debian workstation to an address in that subnet. But you won't be able to see all the bootup messages and it will make debugging/controlling the router more difficult. With the serial connection, you can see the bootloader etc.

1. 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
```

2. Run `minicom` on your Debian workstation to connect to the router, using the USB device from above.
3. Your console should appear similar to figure 1.2.

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

1.2. INITIAL CONFIGURATION



Figure 1.3: pfSense `minicom` Settings

4. The connection settings are 115200 bps, 8N1, no Hardware Flow Control, no Software Flow Control. Note, Hardware Flow Control is on by default and may prevent you from entering text into the console.
5. To change these settings in `minicom`, hit `ctrl-a` then the letter `o`.
6. In the menu, with the arrow keys, select `Serial port setup`.
7. Set the values listed in figure 1.3.
8. Plug in power to the pfSense router, and watch it boot up in `minicom`. It takes 1 minute, 20 seconds for a pfSense model SG-4860 firewall to cold boot with a default configuration.
9. In the pfSense menu, select 1) Assign Interfaces. See console listing below.

```
*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense
↪ ***

WAN (wan)      -> igb1      ->
LAN (lan)      -> igb0      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> igb2      ->
OPT2 (opt2)    -> igb3      ->
OPT3 (opt3)    -> igb4      ->
OPT4 (opt4)    -> igb5      ->

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
```

```
6) Halt system          15) Restore recent configuration
7) Ping host           16) Restart PHP-FPM
8) Shell
```

Enter an option: 1

Valid interfaces are:

```
igb0  00:08:a2:00:00:00  (up) Intel(R) PRO/1000 Network Connection,
      ↳ Version -
igb1  00:08:a2:00:00:01 (down) Intel(R) PRO/1000 Network Connection,
      ↳ Version -
igb2  00:08:a2:00:00:02 (down) Intel(R) PRO/1000 Network Connection,
      ↳ Version -
igb3  00:08:a2:00:00:03 (down) Intel(R) PRO/1000 Network Connection,
      ↳ Version -
igb4  00:08:a2:00:00:04 (down) Intel(R) PRO/1000 Network Connection,
      ↳ Version -
igb5  00:08:a2:00:00:05 (down) Intel(R) PRO/1000 Network Connection,
      ↳ Version -
```

Do VLANs need to be set up first?

If VLANs will not be used, or only for optional interfaces, it is
↳ typical to
say no here and use the webConfigurator to configure VLANs later, if
↳ required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(igb0 igb1 igb2 igb3 igb4 igb5 or a): igb1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(igb0 igb2 igb3 igb4 igb5 a or nothing if finished): igb0

Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection
(igb2 igb3 igb4 igb5 a or nothing if finished):

The interfaces will be assigned as follows:

```
WAN  -> igb1
LAN  -> igb0
```

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!

1.2. INITIAL CONFIGURATION

10. Note the MAC address for the LAN interface.
11. Copy MAC address to main DHCP/DNS server, and reserve IP address. In other words, set up this new firewall on the local LAN DHCP server (if available).
12. Set DHCP for WAN. This is assuming the WAN is on an interface with DHCP (e.g. cable modem). If it is statically set, set the address here.
13. Disable IPv6. the address here.
14. In the pfSense menu, select 2) Set interface(s) IP address,
15. Then 1 to select the WAN interface. See console listing below.

```
Enter an option: 2

Available interfaces:

1 - WAN (igb1 - dhcp, dhcp6)
2 - LAN (igb0 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

The IPv4 WAN address has been set to dhcp

Press <ENTER> to continue.
```

16. Set static IP for LAN, using 10.72.9.254/24 as an example.
17. Do not set an IPv6 address.
18. Don't enter a gateway.

19. Don't enable DHCP server (for now, at least).
20. In the pfSense menu, select 2) Set interface(s) IP address.
21. Then 2 to select the LAN interface. See console listing below.

```
Enter an option: 2

Available interfaces:

1 - WAN (igb1 - dhcp)
2 - LAN (igb0)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.72.9.254

Subnet masks are entered as bit counts (as in CIDR notation) in
→ pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0    = 16
      255.0.0.0      = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.72.9.254/24
You can now access the webConfigurator by opening the following URL
→ in your web browser:
https://10.72.9.254/

Press <ENTER> to continue.
```

1.2.3 Initial Wizard Setup via Web Browser

1. If needed, set IP address on Debian workstation that is in the same subnet as new firewall. If you have two ethernet interfaces, and the new firewall is plugged into the second ethernet interface, depending on the interface name, run one of:

```
ifconfig eth0 10.72.9.12
ifconfig eth1 10.72.9.12
ifconfig enp3s0 10.72.9.12
```

If your workstation has only one ethernet connection and the new firewall is plugged into a switch that connects to the workstation, set a second IP address on the primary ethernet interface. It will likely be this:

```
ifconfig eth0:0 10.72.9.12
```

2. On your Debian workstation, point your browser to the IP address you set on the LAN interface. For example, <https://10.72.9.254/>
3. Your browser will issue a warning about the SSL certificate. Don't send to Google...

```
Your connection is not private

Attackers might be trying to steal your information from 10.72.9.254
    ↳ (for example, passwords, messages, or credit cards).
    ↳ NET::ERR_CERT_AUTHORITY_INVALID
```

4. In your browser hit Advanced, which will display this text (see also figure 1.4):

```
This server could not prove that it is 10.72.9.254; its security
    ↳ certificate is not trusted by your computer's operating system.
    ↳ This may be caused by a misconfiguration or an attacker
    ↳ intercepting your connection.
```

Proceed to 10.72.9.254 (unsafe)

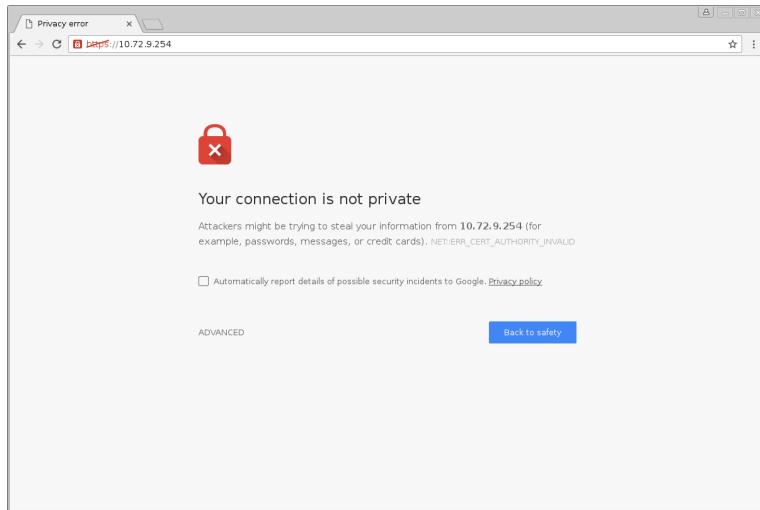


Figure 1.4: pfSense Cert Authority Invalid

5. Click **Proceed** to go through with this operation. A new SSL cert will be set up on the firewall in later steps to replace this self-signed certificate.
6. Log in to firewall (e.g. <https://10.72.9.254>). The initial username is **admin** and the password is **pfsense**, as seen in figure ??.
7. Start Wizard (figure 1.6), hit **Next**.
8. pfSense Gold plea, see (figure 1.7), hit **Next**.
9. This is the **General Information** page of the wizard, see figure 1.8.
10. Set **Hostname**, in this example **fw729**. Select a different hostname than fw729.
11. Set **Domain**, in this example **alephobjects.com**.
12. **Primary DNS Server** and **Secondary DNS Server** can be blank for now. They will be set it later steps.
13. **Override DNS**, leave checked.

1.2. INITIAL CONFIGURATION

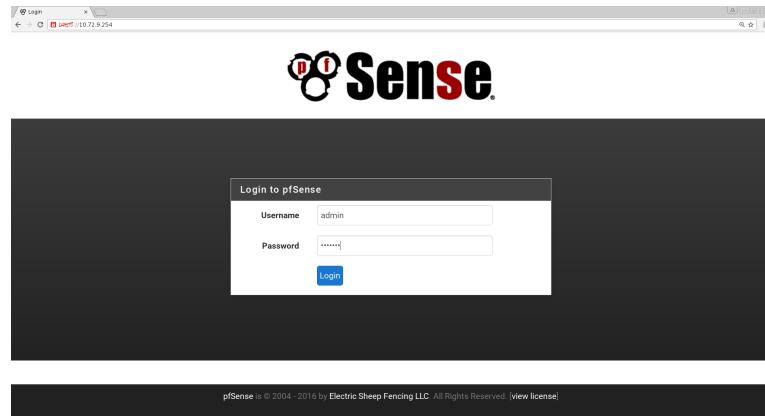


Figure 1.5: pfSense Login

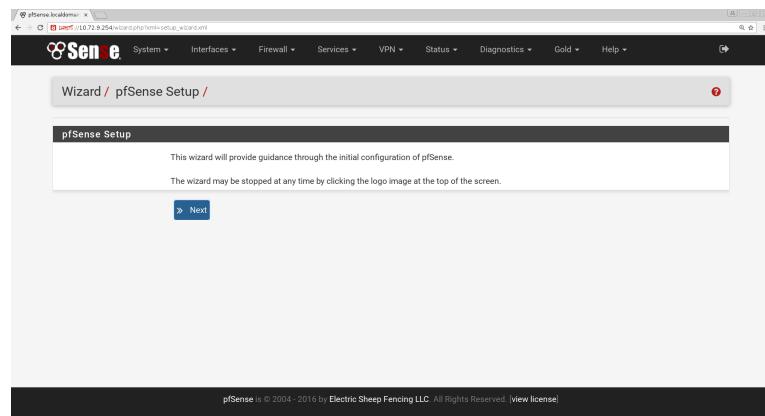


Figure 1.6: pfSense Wizard

14. Hit **Next** to save.
15. The **Time Server Information** page of the wizard, see figure 1.9.
16. **Time Server Hostname**, leave at default.
17. Set **Timezone** to **America/Denver**.
18. Hit **Next** to save.

pfSense

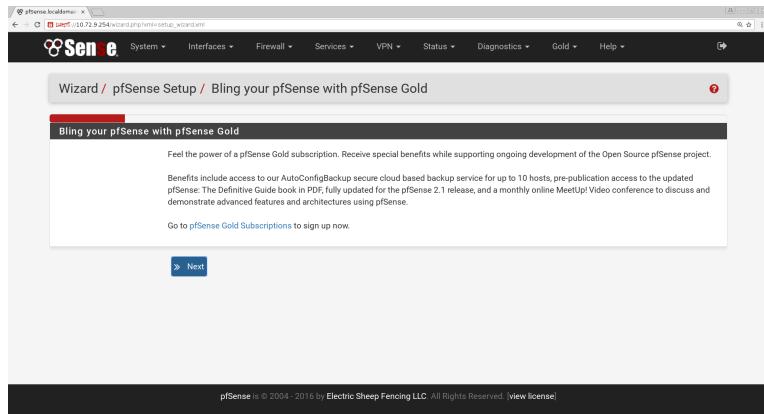


Figure 1.7: pfSense Gold

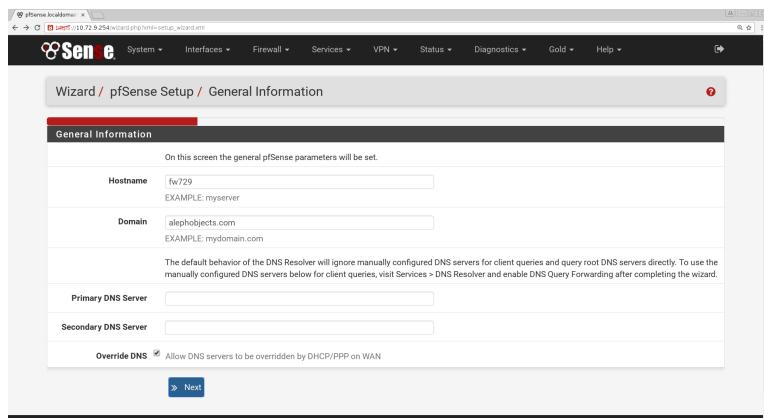


Figure 1.8: pfSense Wizard General Information

19. The **Configure WAN Interface** page of the wizard, see figure 1.10.
20. Configure WAN interface. Leave the WAN interface ethernet cable unplugged. In later steps, once we get the basic firewalling etc. running, we can plug in WAN and configure it. For now, take the WAN DHCP defaults.
21. See figure 1.10.

1.2. INITIAL CONFIGURATION

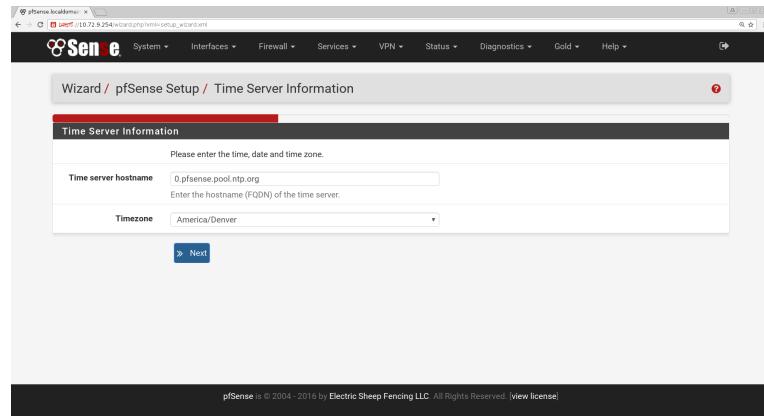


Figure 1.9: pfSense Wizard Timezone

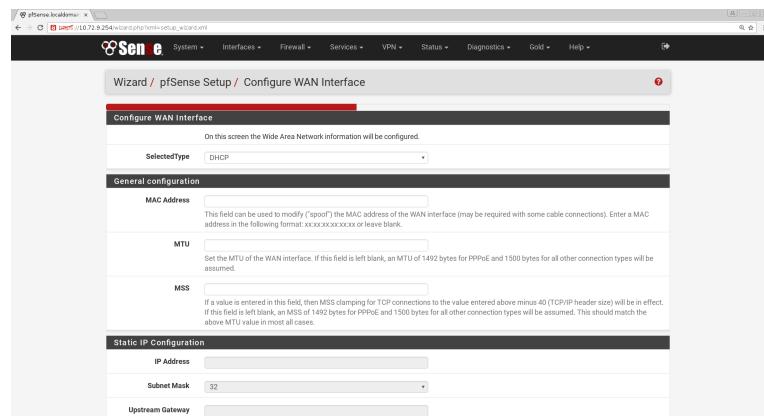


Figure 1.10: pfSense Wizard WAN Configuration

22. Selected type use DHCP.
23. MAC Address, leave blank.
24. MTU, leave blank.
25. MSS, leave blank.
26. MAC Address, leave blank.

27. Hit **Next** to save.
28. Configure LAN interface.

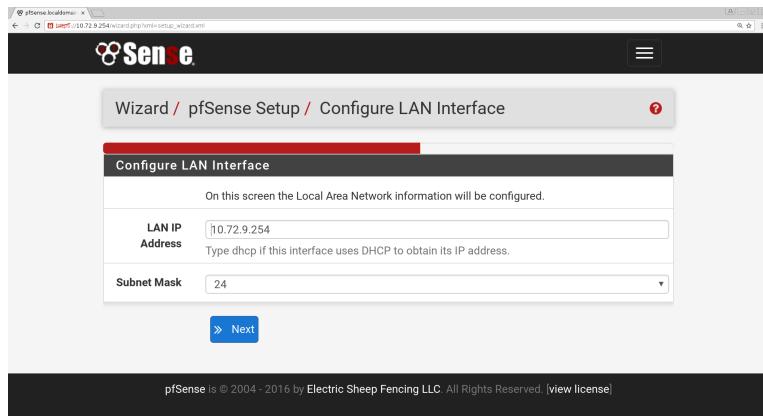


Figure 1.11: pfSense Wizard LAN Configuration

29. The **Configure LAN Interface** page of the wizard, see figure 1.11.
30. **LAN IP Address**, set the static IP. In this example **10.72.9.254**.
31. **Subnet Mask**, set to **24**, which is **255.255.255.0**.
32. Hit **Next** to save.
33. Set **Admin WebGUI Password**, see figure 1.12.
34. Choose something unique and following good practices. Use a good password generator.
35. Hit **Next** to save.
36. Hit **Reload** to use the new configuration.
37. Watch wizard reload. This should take less than a minute.
38. The wizard is now complete. Click **here** in **Click here to continue on to pfSense webConfigurator**.

1.2. INITIAL CONFIGURATION

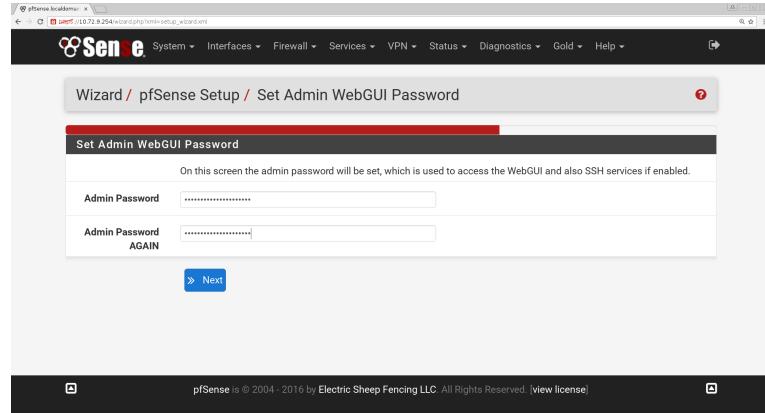


Figure 1.12: pfSense Wizard Admin Password

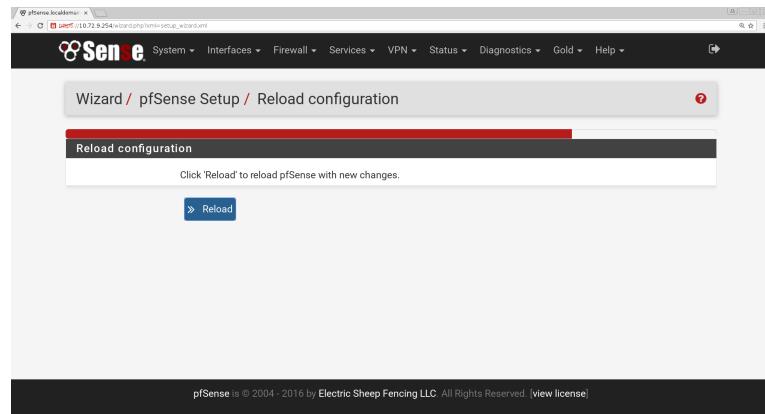


Figure 1.13: pfSense Wizard Reload Configuration

1.2.4 Initial Dashboard

The main dashboard gives an overview of the system. It will be configured more in later steps.

pfSense

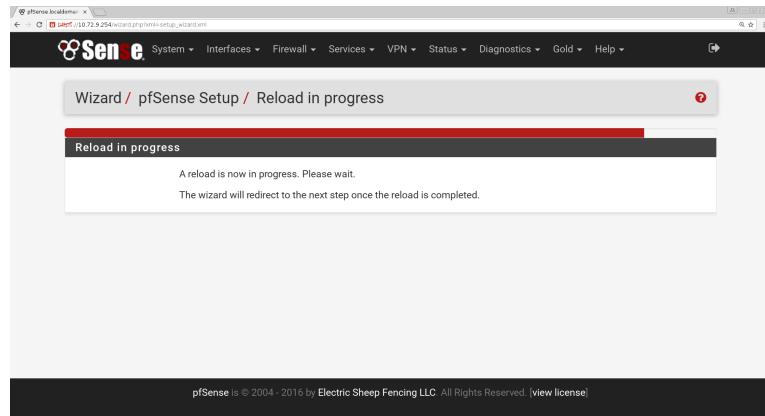


Figure 1.14: pfSense Wizard Reloading

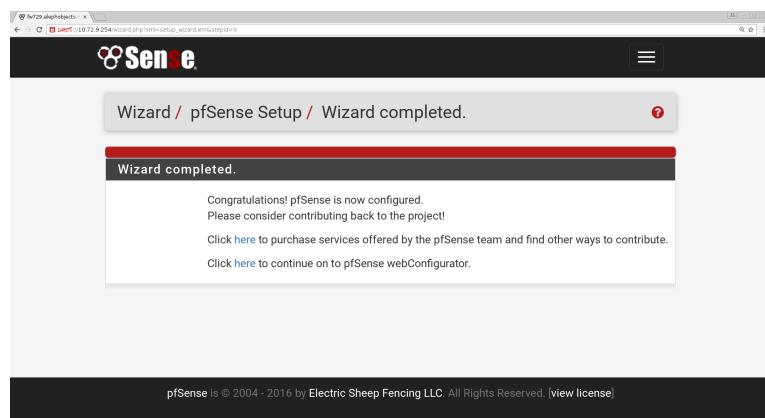


Figure 1.15: pfSense Wizard Complete

1.2.5 Moar Configuration

Now that the basic setup of the firewall is done...there is more... Upon logging in the first time, you are greeted with a basic Dashboard. Menu items are across the top. See figure 1.16.

1.2. INITIAL CONFIGURATION

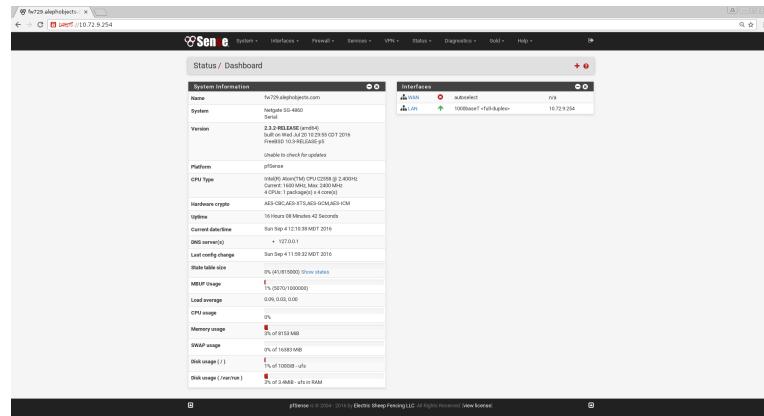


Figure 1.16: pfSense Initial Dashboard

1.2.6 Set Up a New User

1. Go to the top **System** tab and click **User Manager**.

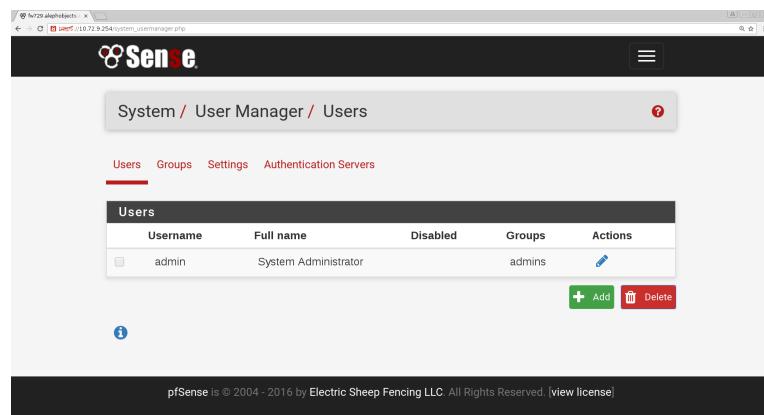


Figure 1.17: pfSense Menu: System, User Manager, Users

2. Click Add.
3. Add **Username**, jebba in this example—use something else.
4. Add a good, well-generated unique password.

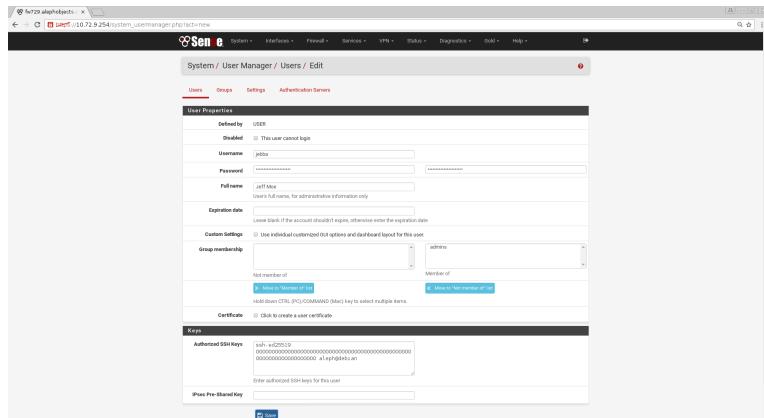


Figure 1.18: pfSense Menu: System, User Manager, Add User

5. Enter the user's **Full name**.
6. **Expiration date** leave blank.
7. Move to add to **Group membership admins**.
8. **Certificate**, leave blank for now (one will be set up later with OpenVPN).
9. For **Authorized SSH Keys**, add your SSH key from your Debian workstation. It will be either `/home/aleph/.ssh/id_ed25519.pub` or for older keys `/home/aleph/.ssh/id_rsa.pub`. Be sure the file ends in `.pub` and isn't the private key. You can use multiple keys, one per line.
10. Hit **Save**.
11. Log out as the admin user by clicking the logout icon in the upper right corner of the pfSense web page.
12. Log back in as the newly created user and password in the above steps.

1.2. INITIAL CONFIGURATION

```
last pid: 88064;  load averages: 0.00, 0.00, 0.00    up 0+17:45:38 13:47:34
48 processes: 2 running, 46 sleeping
CPU: 0.0% user, 1.1% nice, 2.0% system, 0.0% interrupt, 96.9% idle
Mem: 36M Active, 65M Inact, 186M Wired, 116M Buf, 7605M Free
Swap: 16G Total, 16G Free

```

PID	USERNAME	THR	PRI	NICE	SIZE	RES	STATE	C	TIME	WCPU	COMMAND
38495	root	1	20	0	14408K	1952K	select	1	0:05	0.00%	powerd
66180	root	2	20	0	30144K	17988K	usem	3	0:02	0.00%	ntpd
35726	root	1	-52	r0	6244K	2212K	nanslp	0	0:02	0.00%	watchdogd
70566	unbound	4	20	0	59492K	19448K	kqread	3	0:01	0.00%	unbound
269	root	1	20	0	262M	25064K	kqread	0	0:01	0.00%	php-fpm
9592	root	1	20	0	16676K	2088K	bpf	0	0:01	0.00%	filterlog
76039	root	1	21	0	262M	36424K	accept	1	0:00	0.00%	php-fpm
78014	root	1	20	0	14520K	2320K	select	3	0:00	0.00%	syslogd
76605	root	1	20	0	39136K	7372K	kqread	0	0:00	0.00%	nginx
79201	root	1	52	20	17000K	2556K	wait	1	0:00	0.00%	sh
16059	root	1	20	0	16532K	2208K	nanslp	1	0:00	0.00%	cron
73359	jebba	1	20	0	21856K	2972K	CPU3	3	0:00	0.00%	top
2155	jebba	1	20	0	17340K	3688K	pause	1	0:00	0.00%	tcsh
2063	jebba	1	20	0	63736K	7592K	select	2	0:00	0.00%	sshd
1812	root	1	32	0	63736K	7256K	select	1	0:00	0.00%	sshd
78808	root	1	20	0	39136K	6964K	kqread	0	0:00	0.00%	nginx
79217	root	1	20	0	39136K	6964K	kqread	2	0:00	0.00%	nginx

Figure 1.19: pfSense Via SSH, Running `top`

1.2.7 SSH Access

At this point, enough is set up in the router to allow for remote SSH access. Log in, like in this example, where the port is 2222, the user is `jebba`, and the IP address of the firewall is `10.72.9.254`. Side note: the FreeBSD shell displays better on a black terminal than a white one.

```
ssh -p 2222 jebba@10.72.9.254
```

Some example commands to run:

```
top # use q to exit
dmesg
df -h
ps ax
ifconfig
ping -c 1 10.72.9.254
route -n show 0.0.0.0 # Will give error if no gateway is set
# etc...
```

1.2.8 Admin Access Configuration

1. Goto System -> Advanced, Admin Access tab.

pfSense

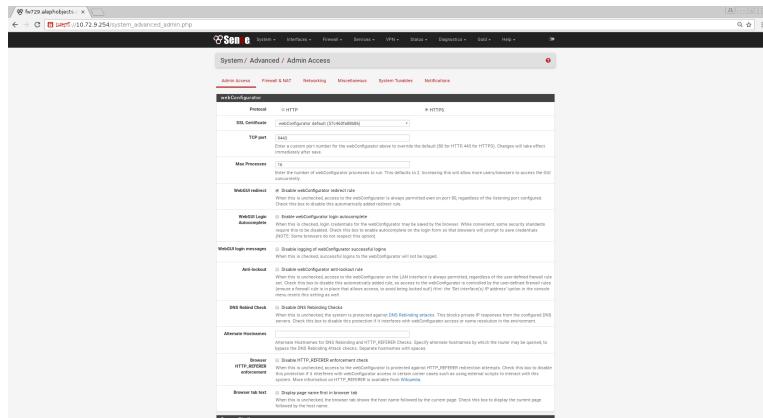


Figure 1.20: pfSense Menu: System, Advanced, Admin Access

2. Leave **Protocol** at **HTTPS**.
3. Set **TCP port** to randomish port between 1 and 65535. This will be the new pfSense web interface port address.
4. Set **Max Processes**: 16 (2 is too low, not sure what is ideal).
5. Check **WebGUI redirect** to disable port 80.
6. Leave **WebGUI Login Autocomplete** unchecked.
7. Leave **WebGUI login messages** unchecked.
8. Leave **Anti-lockout** unchecked.
9. Leave **DNS Rebind Check** unchecked.
10. Leave **Alternate Hostnames** blank. If there are known other names for the firewall, they can be entered here.
11. Leave **Browser HTTP_REFERER enforcement** unchecked.
12. Leave **Browser tab text** unchecked.
13. Check **Secure Shell Server** to enable SSH.
14. Check **Authentication Method** to disable password logins.

1.2. INITIAL CONFIGURATION

15. Set **SSH Port** to a new randomish port between 1 and 65535.
16. Leave **Serial Speed** at 115200.
17. Check **Console menu** to password protect the serial console menu.
18. Hit **Save**.
19. If a new port was set, the browser will redirect to it after a few seconds, for example to https://10.72.9.254:9443/system_advanced_admin.php
20. At this point, you can optionally SSH into the firewall, if a key was set up for the user.

1.2.9 Advanced Networking Configuration

Note, the **System -> Advanced, Firewall & NAT** section can be left at defaults.

Turn off IPv6 and network hardware processing for Suricata. See figure [1.21](#).

1. Under **System -> Advanced, Networking** tab.
2. Uncheck **Allow IPv6**, to disable IPv6 (yay!).
3. Check to disable **Hardware Checksum Offloading**. This needs to be disabled for Suricata inline mode. This needs to be disabled when running pfSense inside a virtual KVM, or you'll get TCP/IP checksum errors.
4. Check to disable **Hardware TCP Segmentation Offloading**. This needs to be disabled for Suricata inline mode.
5. Check to disable **Hardware Large Receive Offloading**. This needs to be disabled for Suricata inline mode.
6. Hit **Save**.

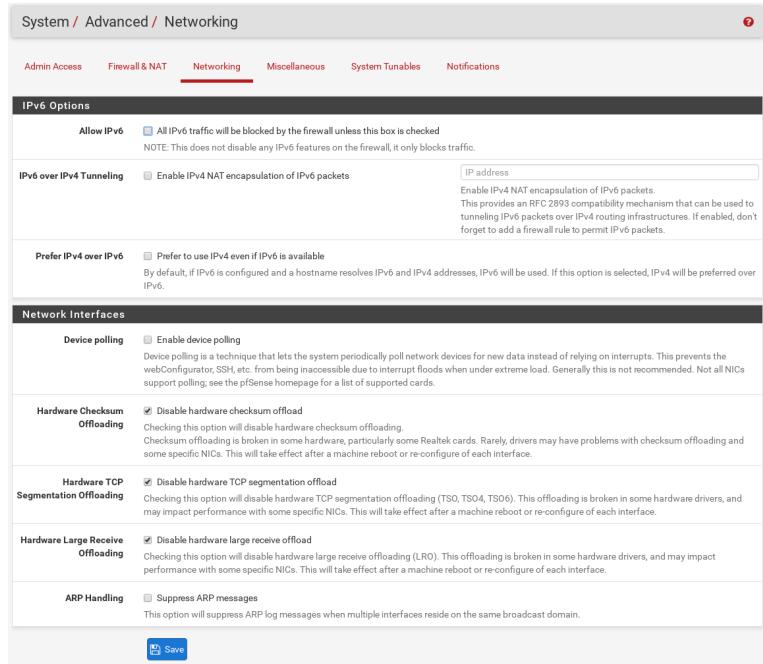


Figure 1.21: pfSense Menu: System, Advanced, Networking

1.2.10 Advanced Miscellaneous Configuration

Miscellaneous configuration, such as hardware accelerated crypto. See figure 1.22.

1. System → Advanced, Miscellaneous.
2. Cryptographic Hardware should be set to AES-NI for any hardware from pfSense. For other hardware, check dmesg.
3. Thermal Sensors: use Intel Core* CPU on-die thermal sensor.
4. Hard disk standby time, set to 6 minutes (not sure this really has any effect).
5. Host UUID, check Do NOT send HOST UUID with user agent.
6. Take defaults for everything else.
7. Hit Save.

1.2. INITIAL CONFIGURATION



Figure 1.22: pfSense Menu: System, Advanced, Miscellaneous

1.2.11 Advanced Notifications Configuration

Notifications configuration, disable. See figure 1.23

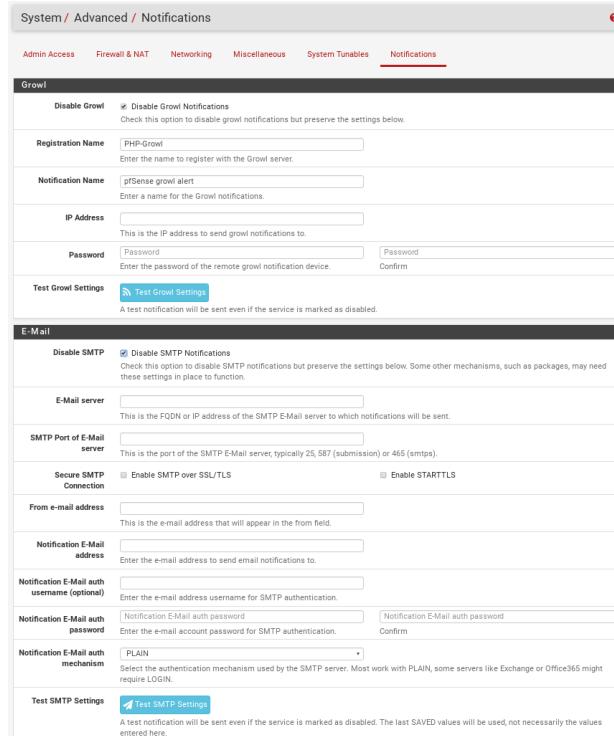


Figure 1.23: pfSense Menu: System, Advanced, Notifications

1. System → Advanced, Notifications.
2. Check to Disable Growl Notifications
3. Check to Disable SMTP.
4. Hit Save.

1.2.12 SSL Create a Certificate Signing Request

A new SSL certificate will be created in the following steps. This certificate will then be used to encrypt web administration sessions ([https](https://)).

1. System → Cert. Manager, Certificates.
2. Click Add.

1.2. INITIAL CONFIGURATION

3. Method: Create a Certificate Signing Request.
4. Descriptive Name, use the hostname of the firewall being setup.
5. Key length: 4096. That may be overkill, but it is just used for the CSR so it doesn't matter.
6. Digest Algorithm: sha512.
7. Country Code: US.
8. State: Colorado.
9. City: Loveland.
10. Common name, use hostname of firewall.
11. Hit Save.

1.2.13 SSL Retrieve and Submit a Certificate Signing Request

1. System -> Cert. Manager, Certificates.
2. For the new cert added above, click Export Request mini-icon.
3. Go to the SSL provider, such as <https://gandi.net>.
4. Gandi: Standard SSL, single address, 3 year.
5. Paste in the CSR exported from the mini-icon into Gandi.
6. Select Apache/ModSSL for Software used in Gandi,
7. If it says the correct Main domain (CN), hit Submit in Gandi.
8. Delete any temporary *.req file that was downloaded by browser.
9. Gandi: Validation by email (probably). It will take 10+ minutes to get verification back from Gandi (not instant).
10. When verification email arrives, go to the URL provided and enter the provided random string.
11. It takes around 5 minutes for the confirmation to be pushed back to Gandi and make the certificate valid. Wait.

1.2.14 SSL Install New Certificate

1. System -> Cert. Manager, Certificates.
2. When cert is ready and confirmed at Gandi, hit Get the Certificate.
3. Hit the Update CSR pencil on the appropriate certificate line.
4. In the Gandi popup window, copy the certificate data.
5. In the pfSense window, paste the Gandi cert into the Final certificate data field.
6. Delete any downloaded copies.

1.2.15 SSL Import Gandi Certificate Authority

Note, this has to be done after the above Gandi certificate is added to the firewall.

XXX Note, we could also import AO's key here.

1. System -> Cert. Manager, CAs.
2. Under CAs, click Add.
3. Method: Import an existing Certificate Authority.
4. Descriptive Name: GandiStandardSSLCA2.
5. Download the cert from <https://www.gandi.net/static/CAs/GandiStandardSSLCA2.pem>
6. Paste downloaded Gandi certificate into Certificate data.
7. Leave Certificate Private Key blank.
8. Hit Save.

1.2. INITIAL CONFIGURATION

1.2.16 SSL Certificate Revocations

Note, this has to be done after the above Gandi certificate is added to the firewall.

1. **System** → Cert. Manager, Certificate Revocations.
2. Import Certificate Revocations, if any.

1.2.17 General Setup

1. **System** → General Setup.
2. Leave most at defaults.
3. Top Navigation: Fixed (Remains visible at top of page).
4. Hostname in Menu: Hostname only.
5. DNS servers can be bound to particular interfaces here, if needed in multi-WAN (later configuration).
6. Dashboard Columns set to 4.
7. Hit Save.

1.2.18 Use New SSL Certificate for Web Admin

A new SSL certificate was created above. This can now be used by the firewall to encrypt web administration sessions.

1. **System** → Advanced, Admin Access.
2. Change SSL Certificate to the new one created above.
3. Hit Save.
4. Now go to that new hostname with https and the correct port, such as <https://10.72.9.254:9443/>.

1.2.19 Initial Firewall Rules

Some basic firewall rules will be set up now, before the WAN interface is enabled. For now, IPv6 will be rejected on the LAN interface and blocked on the WAN interface.

1. Firewall -> Rules, LAN.
2. LAN interface, click the pencil to edit the IPv6 line.
3. Change Action to Reject.
4. Change Source to any.
5. Change Description to Default Reject LAN IPv6.
6. Hit Save.
7. Hit Apply Changes.
8. Firewall -> Rules, LAN.
9. Click the Copy mini-icon to copy the newly modified IPv6 line.
10. Change Action to Block.
11. Change Interface to WAN.
12. Change Description to Default Block WAN IPv6.
13. Hit Save.
14. Hit Apply Changes.

1.2.20 Initial DNS Resolver Setup

1. Services -> DNS Resolver.
2. Check Enable (default).
3. Network Interfaces: select LAN and localhost.
4. Outgoing Network Interfaces: select WAN, LAN, localhost.

1.2. INITIAL CONFIGURATION

5. Check DHCP Registration
6. Check Static DHCP
7. Hit Save.
8. Hit Apply Changes.
9. Services → DNS Resolver, Advanced Settings.
10. Check Prefetch Support.
11. Check Prefetch DNS Key Support.
12. Increase Message Cache Size to 50 MB or so (?).
13. Hit Save.
14. Hit Apply Changes.

1.2.21 Dynamic DNS Setup

If dynamic DNS is to be set up, follow these steps... XXX

1. Services → Dynamic DNS.

1.2.22 Initial Logging Setup

Setup logging to the local firewall. Remote logging will be set up.

1. Status → System Logs, Settings.
2. Check Forward/Reverse Display.
3. Increase GUI Log Entries to 200.
4. Set Where to show rule descriptions to Display as second row.
5. Note, XXX this is where remote logging will be set up...
6. Hit Save.

1.2.23 Initial Dashboard Setup

1. Status -> Dashboard.
2. Click the Plus + in the upper right corner.
3. Add Firewall Logs.
4. Add Gateways.
5. Add Interface Statistics.
6. Add NTP Status.
7. Add OpenVPN.
8. Add Services Status.
9. Add S.M.A.R.T. Status.
10. Add Thermal Sensors.
11. Add Traffic Graphs.
12. Click the mini-disk icon in the upper right to save the dashboard configuration.

1.2.24 Backup

Make first backup.

1. Diagnostics -> Backup & Restore, Backup.
2. Make a backup and store in the proper location.

1.2.25 Reboot

Now that most of the “initial” setup has been done, reboot to make sure everything comes up clean. It takes less than two minutes to reboot. XXX times.

1. Diagnostics -> Reboot

1.2.26 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**
2. Click to **Edit** the mini pencil icon on the **Gateway** line listed as **Default**.
3. **Monitor IP:** something appropriate upstream, can use **8.8.8.8**.
4. Note: on high latency connections such as satellite, hit **Display Advanced** and increase **Latency thresholds** (default: 750, new: 2500), **Packet Loss thresholds** (15, 25), **Probe Interval** (1000), **Loss Interval** (3000).
5. Hit **Save**.
6. Hit **Apply Changes**.

1.2.27 Update & Install Packages

1. **System** → **Update, System Update**.
2. Check that the **Status** is **Up to date**. If it needs updating, hit **Update**.
3. **System** → **Package Manager, Installed Packages**.
4. The first time here, you need to click on **Available Packages**
5. Wait to download latest package header info.

6. Then go back to **System -> Package Manager, Installed Packages**.
7. If there are any **Installed Packages** that have a **Newer version available**, click the mini icon to **Update** the package. Then **Confirm**.
8. Go to **System -> Package Manager, Available Packages** and install the following packages:
 9. **Cron**.
 10. **ntopng**.
 11. **openvpn-client-export**.
 12. **pfBlockerNG**.
 13. **RRD_Summary**.
 14. **Status_Traffic_Totals**.
 15. **sudo**.
 16. **suricata**.

1.2.28 Set Up **sudo** User

1. **System -> sudo**
2. Add the user added above to sudo.

1.2.29 OpenVPN Certificates

OpenVPN certificates need to be created before OpenVPN can be set up. Also, new DH random seeds are generated.

1. 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

2. System → Cert. Manager. Set up internal certificate authority. XXX
Add Steps
3. System → Cert. Manager. Create internal server certificate. XXX
Add steps

1.2.30 OpenVPN Setup

1. VPN → OpenVPN
2. Set up VPN server.
3. Server Mode: Remote Access (SSL/TLS + User Auth).
4. Backend for Authentication: Local Database (will be FreeRADIUS at some point).
5. Protocol: UDP.
6. Local Port: something randomish. Note for later.
7. Peer Certificate Authority: use the internal CA created earlier.
8. Server Certificate: Use the server certificate created earlier.
9. DH Parameter length (bits): 4096.
10. Encryption Algorithm: AES-256-CBC (256-bit). This algorithm has hardware crypto support on pfSense routers. In pfSense 2.4, AES-256-GCM may be supported and is preferred.
11. Auth digest algorithm: SHA512 (512-bit).
12. Hardware Crypto: BSD Cryptodev engine- RSA, DSA, DH, AES-128-CBC, AES-192-CBC, AES-256-CBC.
13. Certificate Depth: One.
14. Strict User-CN Matching: check Enforce Match once VPN is confirmed working. Leave unchecked for now.
15. IPv4 Tunnel Network: Set the new VPN network.

16. **IPv6 Tunnel Network:** leave blank.
17. **Redirect Gateway:** unchecked.
18. **IPv4 Local network(s):** set the local LAN network, in this case `10.72.9.0/24`.
19. **IPv6 Local network(s):** leave blank.
20. **Compression:** Enabled with Adaptive Compression.
21. **Inter-client communication:** Checked.
22. **Disable IPv6:** Checked.
23. **Dynamic IP:** Unchecked, at least for now.
24. **Topology:** subnet.
25. **DNS Default Domain:** Checked, and set domain.
26. **DNS Server enable:** Checked.
27. **DNS Server 1:** enter servers.
28. Hit Save.

1.2.31 OpenVPN User Certificate Creation

Each user needs their own certificate, which can be tied to their user account on the firewall. Note, FreeRADIUS will be used for user authentication in the future.

XXX this needs to be checked.

1. System -> User Manager
2. Click Add, to create a new VPN user.
3. **Certificate:** Check to create user certificate.
4. **Descriptive name:** enter a `username.domainname`, such as `jebbavpn.alephobjects.com`.
5. **Certificate Authority:** Select internal CA created above.

1.2. INITIAL CONFIGURATION

6. Key length: 2048.
7. Lifetime: 1095.
8. Hit Save.

1.2.32 OpenVPN User Certificate Export

Each user needs their own certificate, which can be tied to their user account on the firewall. Note, FreeRADIUS will be used for user authentication in the future.

XXX this needs to be checked.

1. VPN -> OpenVPN, Client Export
2. Remote Access Server: Select the VPN server created earlier.
3. Verify Server CN: automatic.
4. Block Outside DNS: Checked.
5. At the bottom, export as Standard Configurations, Archive to use with another pfSense server (XXX correct?).
6. To use with OpenVPN in F-Droid (Android), use Inline Configurations (Android).

1.2.33 Turn off Internet via LAN

If the WAN gateway has been set up, disable the LAN gateway.

1. Interfaces -> LAN
2. Change IPv4 Upstream gateway to None.
3. Hit Save.
4. Hit Apply Changes.

1.2.34 Backup

Make another backup.

1. `Diagnostics -> Backup & Restore, Backup.`
2. Make a backup and store in the proper location.

1.2.35 Reboot

Reboot to make sure everything comes up clean.

1. `Diagnostics -> Reboot`

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.

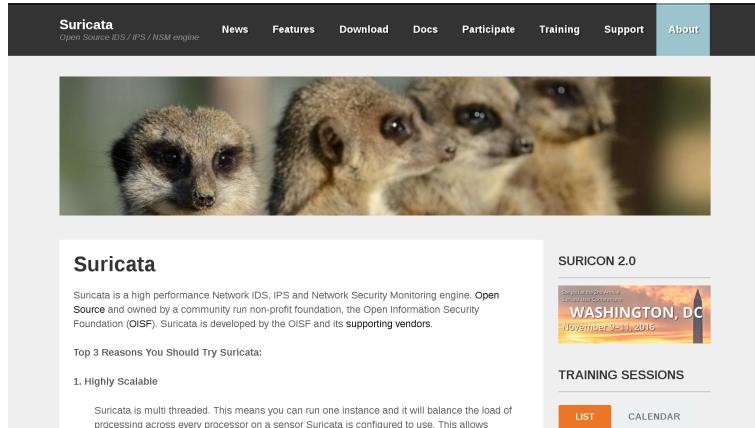


Figure 1.24: Suricata Website

- barnyard2
- 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 1.25: OpenVPN Website

Virtual Private Networks.

1.10. CAPTIVE PORTAL

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.
- 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.

The screenshot shows the official Dnsmasq website. At the top, there is a navigation bar with links for Home, Documentation, Configuration Examples, and Downloads. Below the navigation is a search bar. The main content area features a large title "Dnsmasq" in bold, centered above a brief description of the software's purpose and capabilities. To the left and right of the text are two small, stylized purple and yellow eye icons. A sidebar on the right contains links to various documentation pages like "Introduction", "Configuration", "Usage", etc.

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 caching 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 1.26: 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

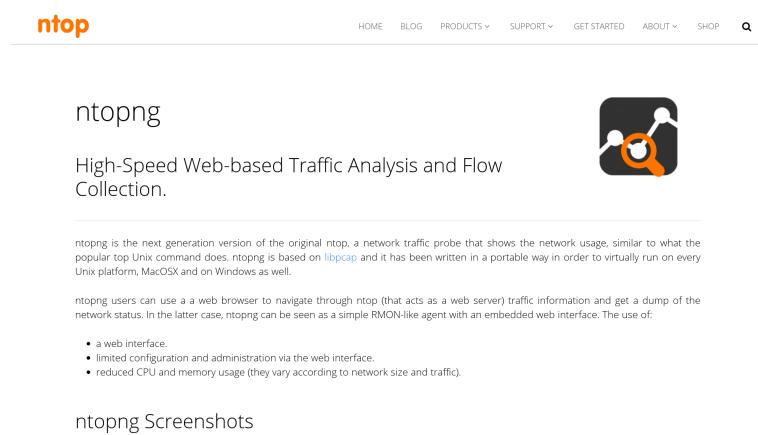


Figure 1.27: ntopng Website

- 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

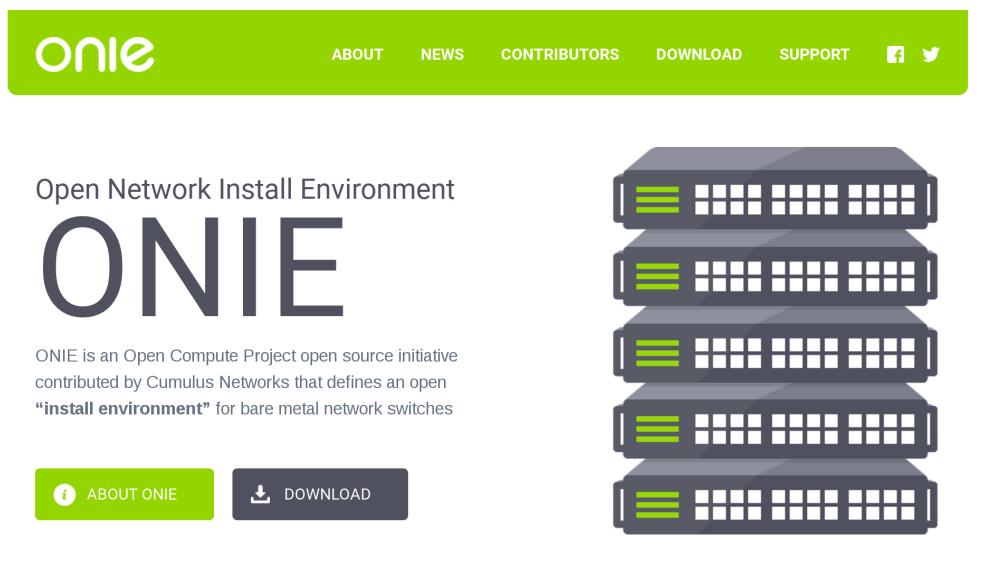


Figure 4.1: ONIE Website

- 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 content area. On the left side of this area, there is a text block describing 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. To the right of the text is a small illustration of a penguin sitting on top of a server rack.

Figure 4.2: Open Network Linux Website

- OpenNSL — May be non-free Broadcom.
- SAI

Forwarding Agents:

- <http://www.quagga.net/> Quagga — “BGP4, BGP4+, OSPFv2, OSPFv3, IS-IS, RIPv1, RIPv2, and RIPng”. In Debian.
- <http://bird.network.cz/> 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

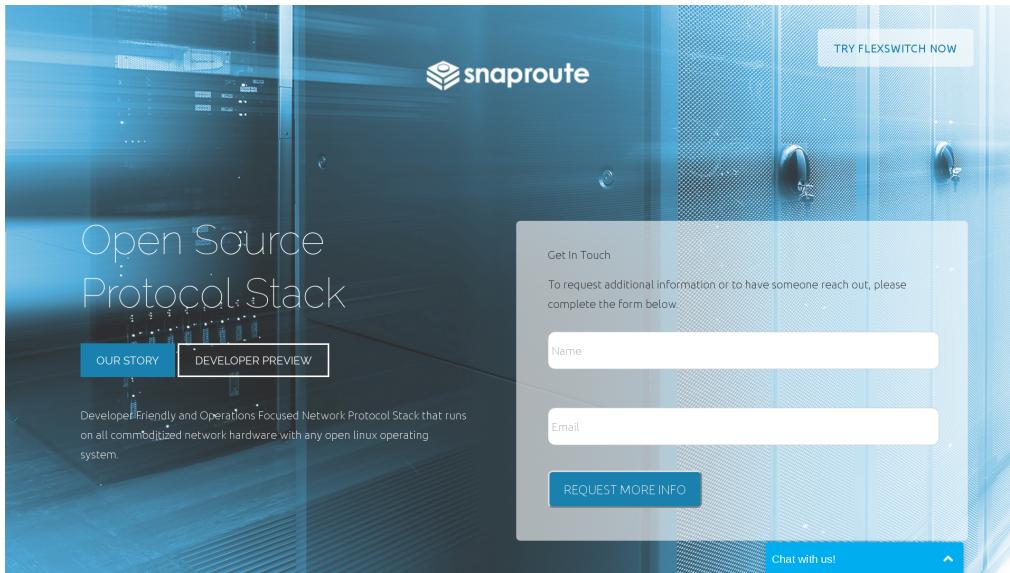


Figure 4.3: Snaproute Website

- 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

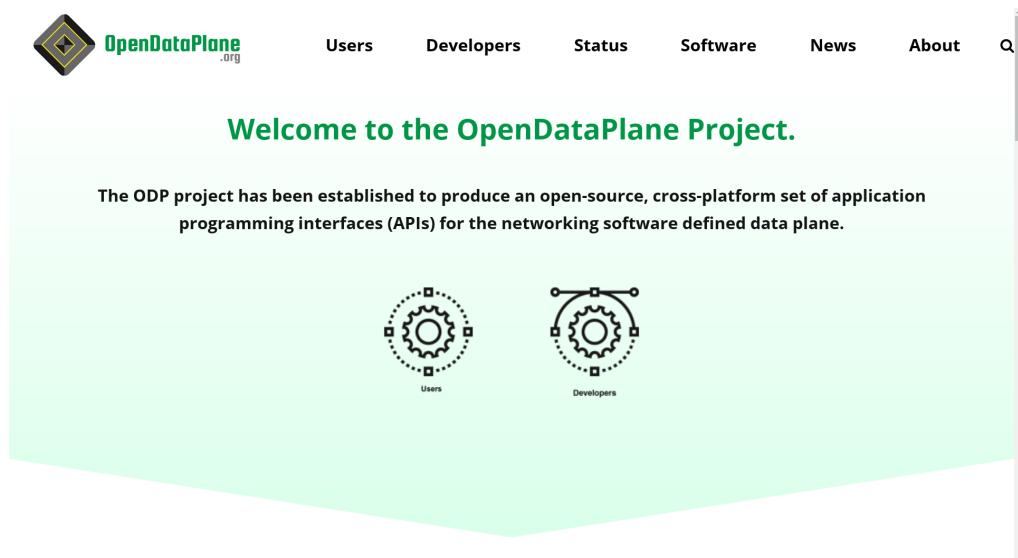


Figure 4.7: OpenDataPlane Website

- 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

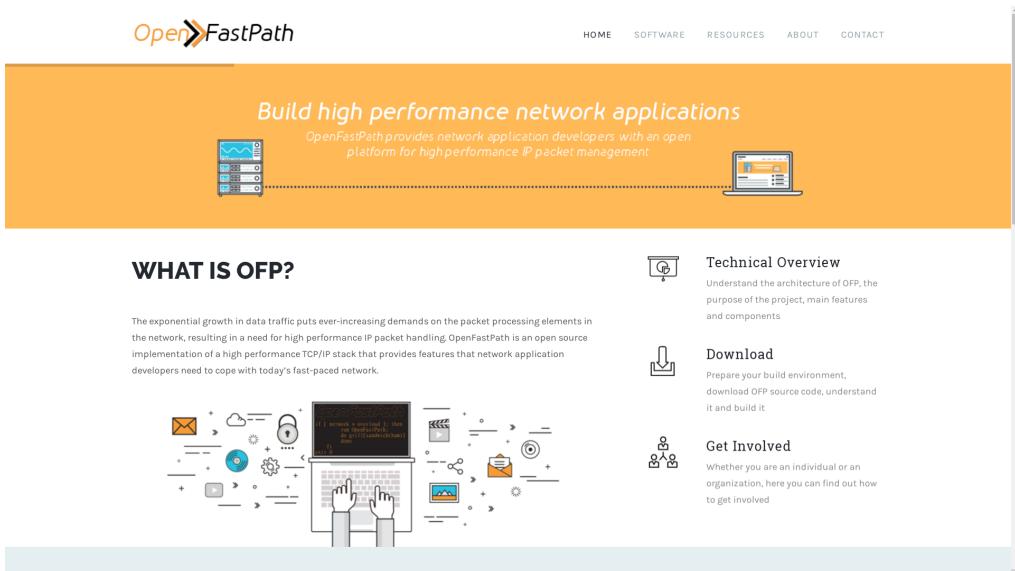


Figure 4.8: OpenFastPath Website

- 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

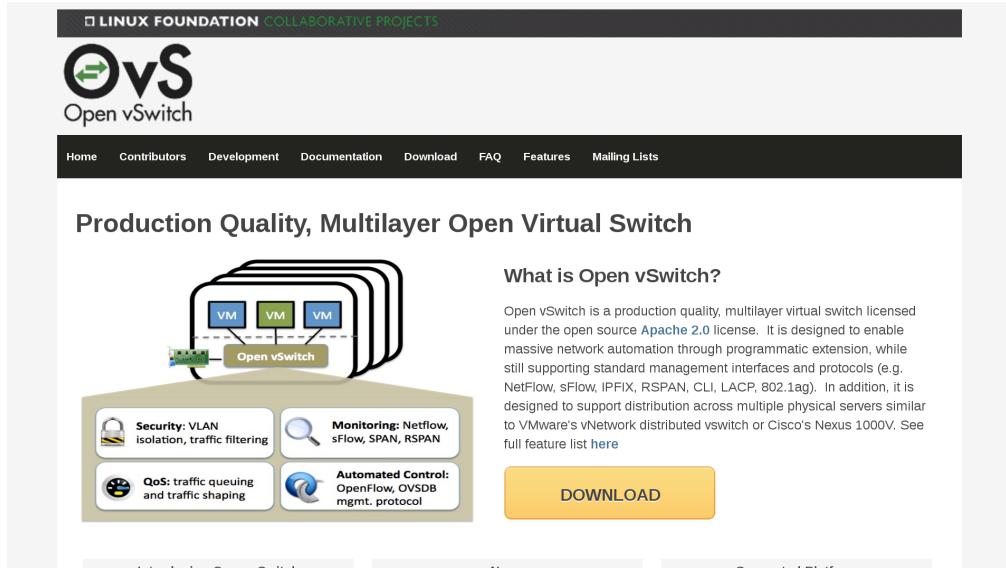


Figure 4.9: Open vSwitch Website

- 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.bigswitch.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

<http://packetpushers.net/sai-and-switchdev-need-to-succeed/> SAI
And Switchdev “SAI and switchdev are hardware abstraction models for switching silicon (ASICs). They are the open source frameworks that allow ASICs to be represented in software. This means you can use a Broadcom ASIC the same way as one from Mellanox or Cavium Xpliant.”

Microsoft's Azure Cloud Switch (ACS) is "Debian Jessie + SAI + everything else needed to power Azure (applications like Quagga, and the switch state service based on Redis)." So their high end switching gear is based on free software, including Quagga and Redis...

4.3 Hardware

Hardware, on which to place free software.

4.3.1 Edge-Core

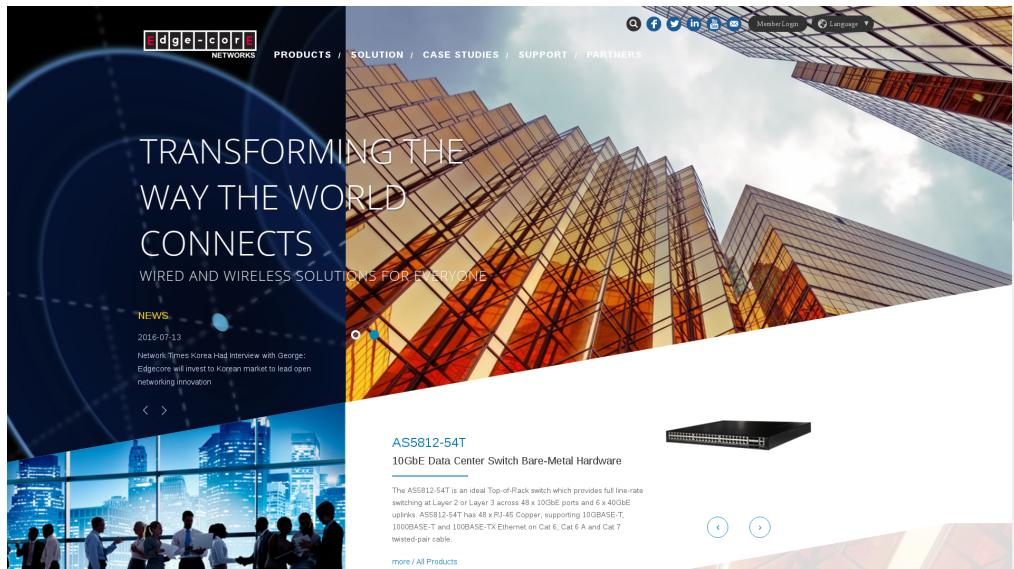


Figure 4.11: Edge-core Website

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

4.3. HARDWARE

4.3.2 Dell

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

Dell makes some bare metal switches that are ONIE compatible.

4.3.3 Netberg

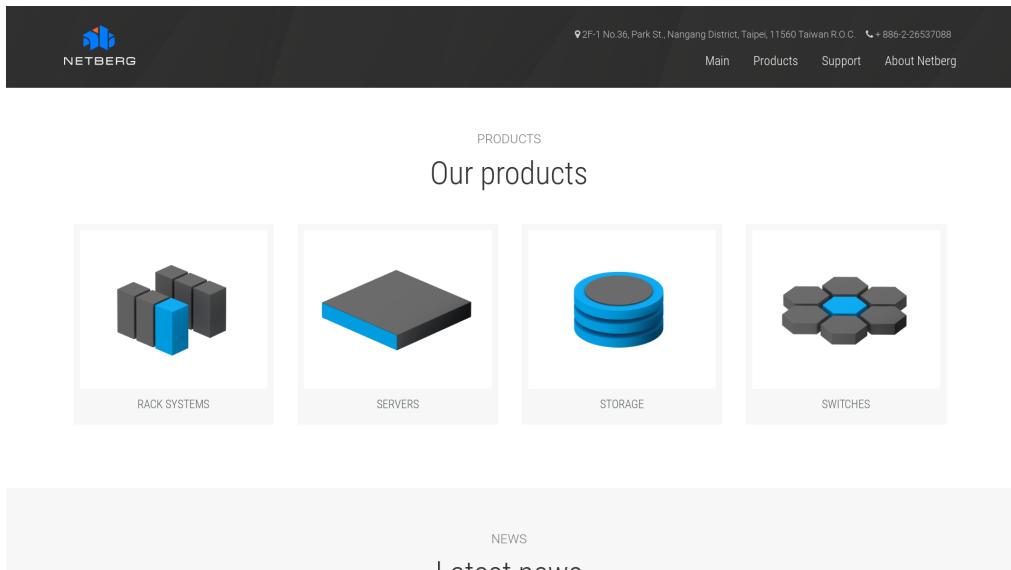


Figure 4.12: Netberg Website

- 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/>

Switches



Figure 4.13: Quanta Website

- Sells "Bare Metal Switches (BMS)"

Uses...Broadcom.

4.3.5 Mellanox

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

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

4.4 Suppliers

4.4.1 White Box

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

4.4. SUPPLIERS



Figure 4.14: Mellanox Website



Figure 4.15: Whitebox Website

1 Gig-e switches available:

Switches

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

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

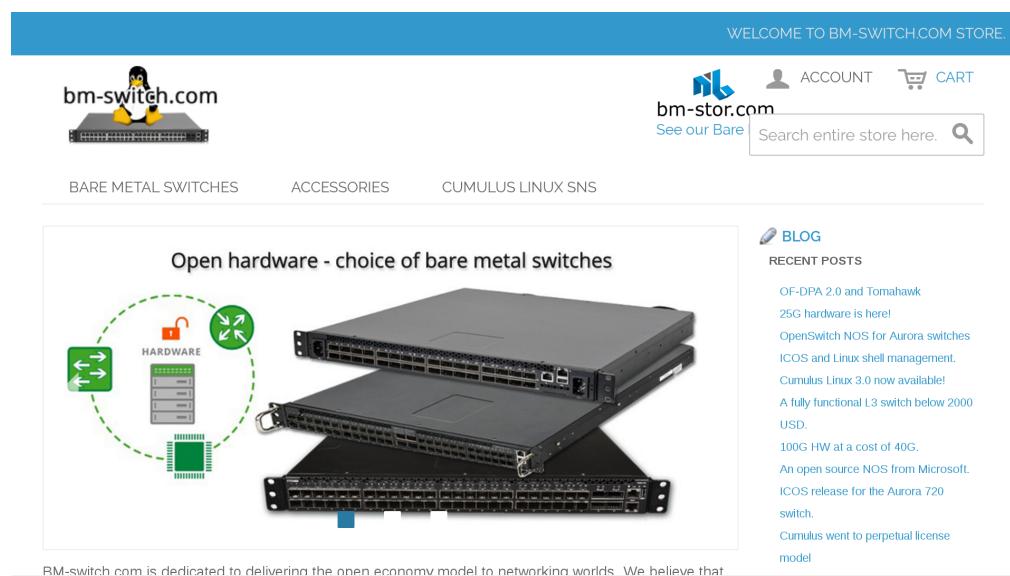


Figure 4.16: Bare Metal Switches Website

- Website:
<https://bm-switch.com/>

4.4. SUPPLIERS

- Reseller of open switches.

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. SUPPLIERS

The screenshot shows the Colfax Direct website. At the top, there's a navigation bar with links for Home, About Us, Contact Us, Search, Checkout, and My Account. A search bar is also present. On the left, there are two columns: 'Browse by Category' and 'Browse by Manufacturer'. The 'Category' column includes links for Adapters, Switches, Cables, NVMe SSDs, SDN Appliance, Gateways, Transceivers, Accessories, Software, Warranty / Support, and Bundles / Specials. The 'Manufacturer' column includes links for Arista, Chelsio, Edgecore (marked as 'new'), Elpues, Emulex, Intel, Mangstor, Mellanox, Myricom, and Netronome (marked as 'new'). The main content area features a yellow banner with the text 'Edgecore Bare Metal Switches' and '10 / 40 / 100 GbE'. Below the banner is a 'BUY NOW' button and a large image of a black network switch. To the right of the switch are five small numbered boxes (1, 2, 3, 4, 5). Below the switch, there's a section titled 'Adapters' with three product cards:

Product	Price
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

On the right side of the page, there are sections for 'Customer Account' (with links for Register/Login), 'Talk to Us' (with links for Got Questions and Need a Quote), and 'Recently Viewed Products' (listing a Picot P-3292 Switch with 48x1GbE Ports with 4x10GbE SFP+ Uplinks, Enhanced TCAM, and a 'Clear List' link).

Figure 4.17: Colfax Direct Website

4.4.4 Penguin Computing

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

Slow manual order/quote process.

OS

Free Operating Systems

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

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?).

- 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.

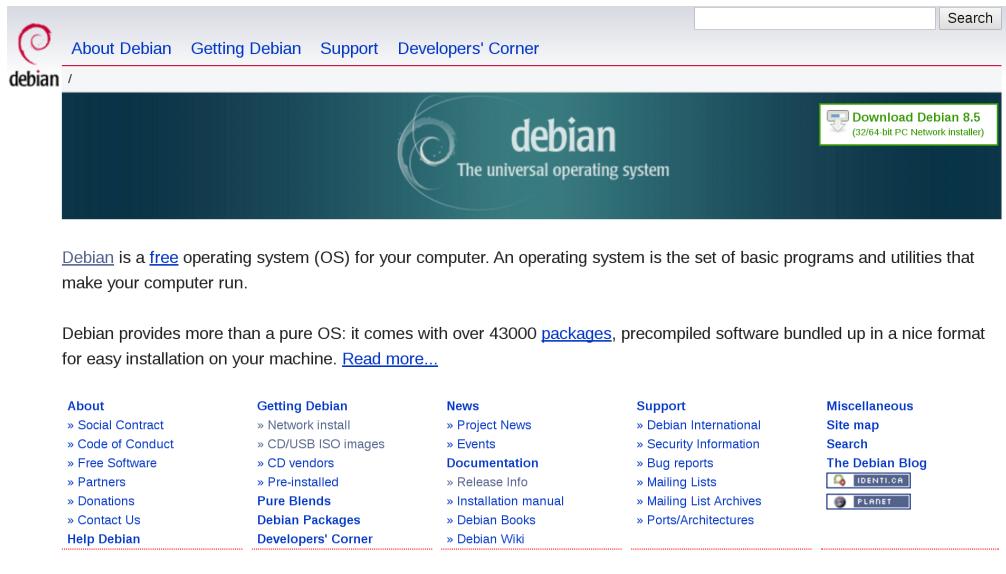


Figure 5.1: Debian Website

- 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 commits.

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

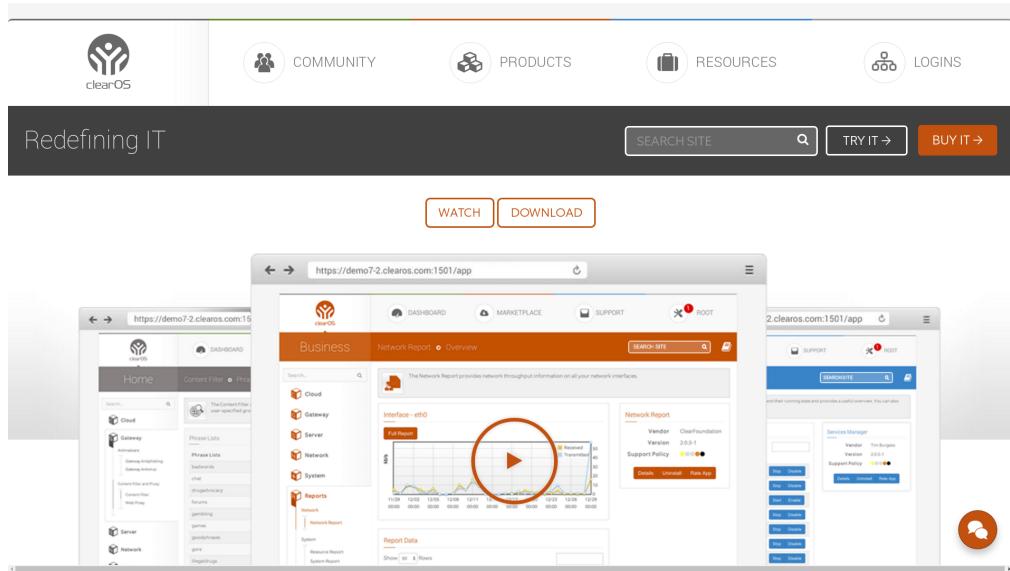


Figure 5.4: clearOS Website

- 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.

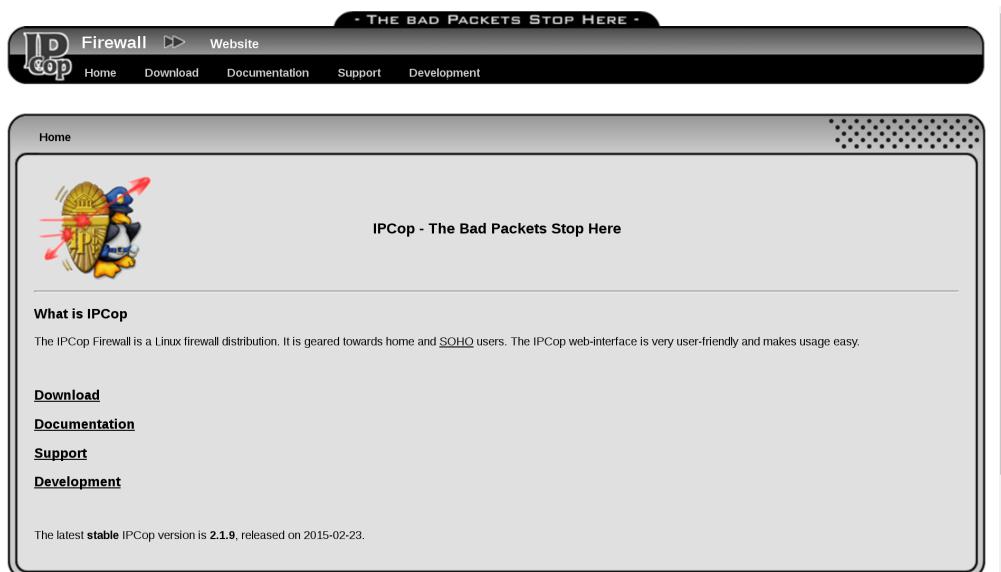


Figure 5.5: IPCop Website

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.
-

5.3. FIREWALLS EVALUATED

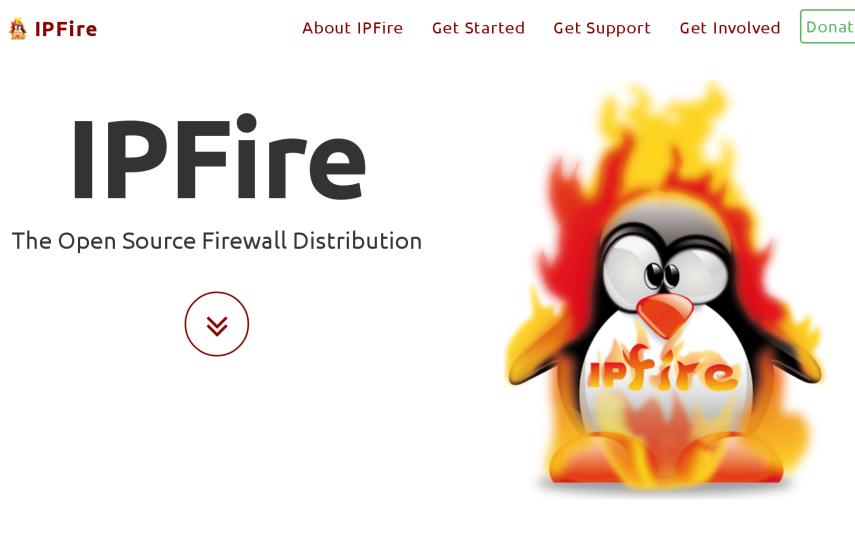


Figure 5.6: IPFire Website

- 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”

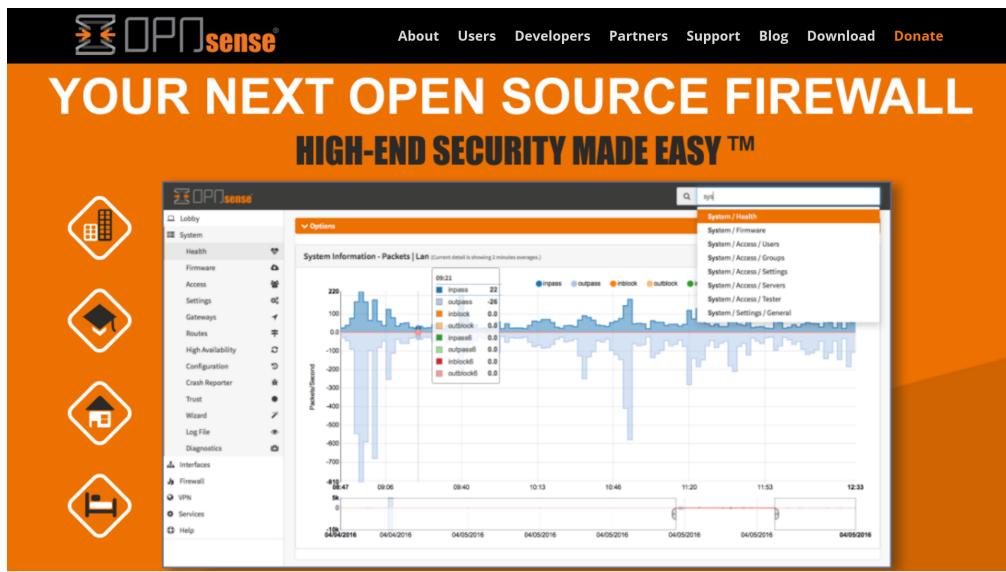


Figure 5.7: OPNsense Website

- 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, looking slightly worried. 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 popular OpenSSH software and the availability of the OS from download sites or as a 3-CD set. The current release is OpenBSD 5.9, released on March 29, 2016. Pre-orders for OpenBSD 6.0 are available at openbsdstore.com. The text also notes that OpenBSD is developed entirely by volunteers, with contributions collected by The OpenBSD Foundation, ensuring the project remains vibrant and free.

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
