Building an OpenBSD Router

Using OpenBSD to make your perfect Firewall / Router.

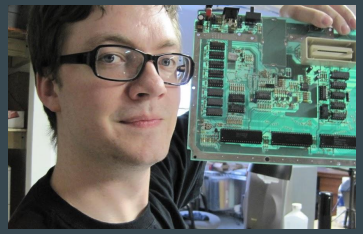
presented by Yukaia and d3c4f

new presentation warning

fancy graphics have been skimped on :(

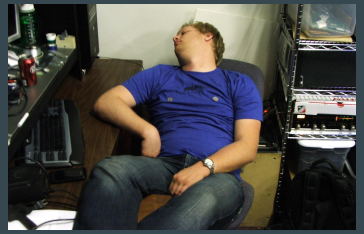
Who?

d3c4f



- Systems Admin / DevOps
- Software Developer
- PortAParty Co-Creator
- theTransistor Founder
- OpenWest Core Team
- BlackHat NOC Team
- Caffeine Addict
- Electronic Badge Designer

Yukaia



- Systems Administrator
- Automobile Enthusiast
- PortAParty Co-Creator
- theTransistor Founder
- OpenWest Core Team
- Blackhat NOC Team
- Dr.Pepper Connoisseur
- Hardware / Server Nerd

Contact Info>

d3c4f@sausage.land

yukaia@sausage.land

What will we be talking about today?

- Why? (why build your own router?, why use OpenBSD?)
- Hardware Requirements
- Installing OpenBSD (a very brief outline)
- Configuring the OS
- Configuring your DHCP Server
- Configuring your DNS Server
- Configuring PF
- Monitoring your traffic / OS / etc.
- Future Updates to your new Router / Firewall

Why?

- Why not use a commercial router?
- Why not use OPNSense / PFSense / Etc?

It just *does*, Mom. I can't explain why it feels so good to be a gangster.

Why not use a commercial router?

Why not use a commercial router?

- Poor updates.
  - Seriously, how often did you update your LinkSys firmware?
  - Updates are always WAY behind the actual distro / BSD they are running on.

Why not use a commercial router?

- Poor updates.
  - Seriously, how often did you update your LinkSys firmware?
  - Updates are always WAY behind the actual distro / BSD they are running on.
- Weak hardware.
  - Most Home / Small business routers have very limited resources.
  - When you build your own, you can scale to the size you need.

Why not use a commercial router?

- Poor updates.
  - Seriously, how often did you update your LinkSys firmware?
  - Updates are always WAY behind the actual distro / BSD they are running on.
- Weak hardware.
  - Most Home / Small business routers have very limited resources.
  - When you build your own, you can scale to the size you need.
- Poor interfaces / Mystery Meat
  - What is it ACTUALLY doing when you click that?

Why not use a commercial router?

- Poor updates.
  - Seriously, how often did you update your LinkSys firmware?
  - Updates are always WAY behind the actual distro / BSD they are running on.
- Weak hardware.
  - Most Home / Small business routers have very limited resources.
  - When you build your own, you can scale to the size you need.
- Poor interfaces / Mystery Meat.
  - What is it ACTUALLY doing when you click that?
- Poor (or non-existent) Logging / Debugging
  - DNS / DHCP / Traffic / Hardware Resource Utilization

Why not use a commercial router?

- Poor updates.
  - Seriously, how often did you update your LinkSys firmware?
  - Updates are always WAY behind the actual distro / BSD they are running on.
- Weak hardware.
  - Most Home / Small business routers have very limited resources.
  - When you build your own, you can scale to the size you need.
- Poor interfaces / Mystery Meat.
  - What is it ACTUALLY doing when you click that?
- Poor (or non-existent) Logging / Debugging
  - DNS / DHCP / Traffic / Hardware Resource Utilization
- Lack of customization
  - DHCP Options? Caching DNS / Traffic? etc.

Why not use a commercial router?

- Security (aside from Updates / Logging / etc)

Why not use a commercial router?

- Security (aside from Updates / Logging / etc)
  - No IDS / IPS available (usually)

Why not use a commercial router?

- Security (aside from Updates / Logging / etc)
  - No IDS / IPS available (usually)
  - Backdoors. That's right, your commercial router is almost certainly backdoored. And don't think the vendor is the only one with knowledge of this.
    - https://tech.slashdot.org/story/14/04/22/001239/intentional-backdoor-in-consumer-routers-found
    - http://securityaffairs.co/wordpress/20941/hacking/netgear-linkys-routers-backdoor.html
    - https://www.wired.com/2013/09/nsa-router-hacking/
    - https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors

Why not use OPNSense / PFSense / etc?

Why not use OPNSense / PFSense / etc?

- Not a bad option at all!
  - Gives you a simple / quick interface to make common changes
  - We actually REALLY like OPNSense!

Why not use OPNSense / PFSense / etc?

- Not a bad option at all!
  - Gives you a simple / quick interface to make common changes
  - We actually REALLY like OPNSense!
- Granularity / Customization / Freedom
  - Maybe you want to know what is actually happening on the backend
  - Maybe you want to install a feature / package / tool that isn't available
  - Maybe you don't like GUIs
  - Maybe you want SQUEEZE every ounce of performance from your hardware
  - Maybe you want to learn more about OpenBSD / PF / etc.

Why OpenBSD?

Why OpenBSD?

- SOLID network stack

Why OpenBSD?

- SOLID network stack
- Awesome security

Why OpenBSD?

- SOLID network stack
- Awesome security
- PF (Packet Filter - Traffic Filtering, NAT/PAT, QoS, and more!)

Why OpenBSD?

- SOLID network stack
- Awesome security
- PF (Packet Filter - Traffic Filtering, NAT/PAT, QoS, and more!)
- Stability!

Why OpenBSD?

- SOLID network stack
- Awesome security
- PF (Packet Filter - Traffic Filtering, NAT/PAT, QoS, and more!)
- Stability!
- ...and more

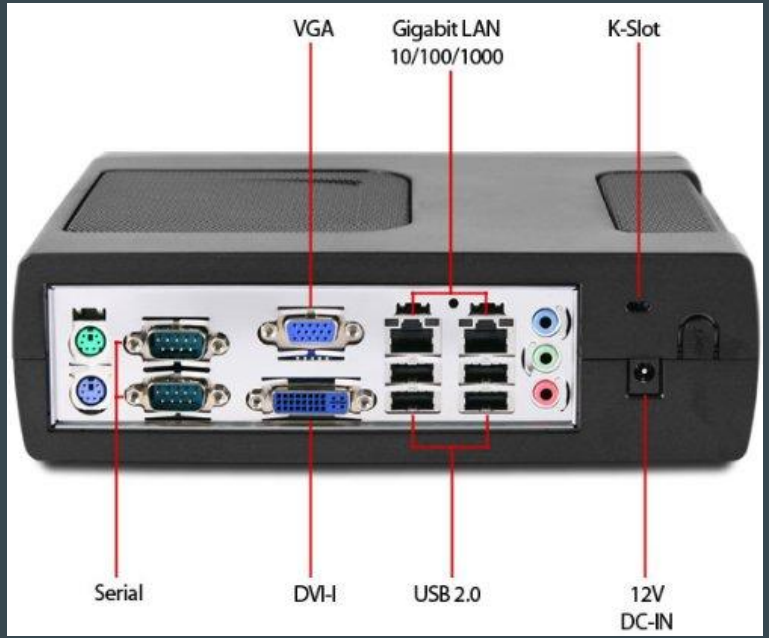
Hardware

Hardware

- Minimum Requirements

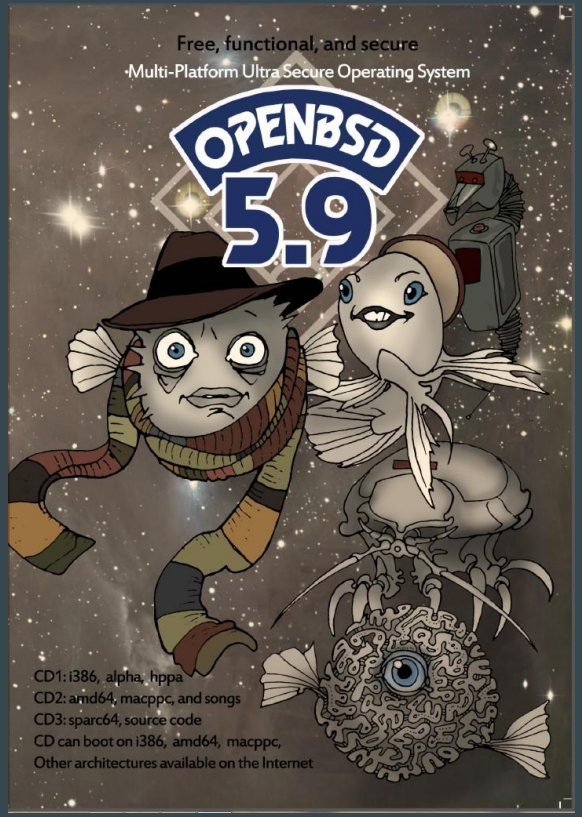
Hardware

- Recommended Minimums
  - Dual Core Atom 800mhz
  - 1GB DDR3
  - At least 2x 100Mbps NICs
    - Verify that the chipset is supported
  - 100 GB Disk Space
    - Spindle Disks will work great
  - Low Power / Low Noise is a Plus :)
- A managed network switch is always nice
  - But not required, by any means

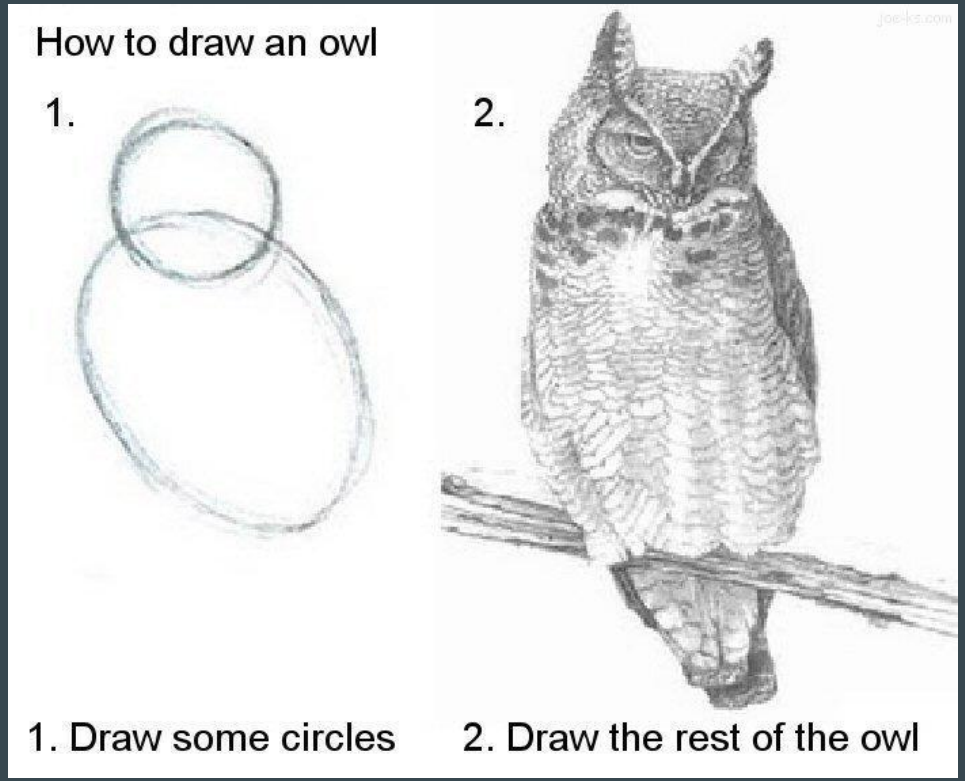


Installing OpenBSD

Installing OpenBSD



Installing OpenBSD



```
cd0(pciide0:1:0): using PIO mode 4, Ultra-DMA mode 2
vga1 at pci0 dev 2 function 0 "InnoTek VirtualBox Graphics Adapter" rev 0x00
vga1: aperture needed
wsdisplay1 at vga1 mux 1: console (80x25, vt100 emulation)
em0 at pci0 dev 3 function 0 "Intel 82540EM" rev 0x02: apic 1 int 19, address 08
:00:27:67:b0:a9
"InnoTek VirtualBox Guest Service" rev 0x00 at pci0 dev 4 function 0 not configu
red
"Intel 82801AA AC97" rev 0x01 at pci0 dev 5 function 0 not configured
ohci0 at pci0 dev 6 function 0 "Apple Intrepid USB" rev 0x00: apic 1 int 22, ver
sion 1.0
"Intel 82371AB Power" rev 0x08 at pci0 dev 7 function 0 not configured
usb0 at ohci0: USB revision 1.0
uhub0 at usb0 "Apple OHCI root hub" rev 1.00/1.00 addr 1
isa0 at mainbus0
pckbc0 at isa0 port 0x60/5 irq 1 irq 12
pckbd0 at pckbc0 (kbd slot)
wskbd0 at pckbd0: console keyboard, using wsdisplay1
softraid0 at root
scsibus1 at softraid0: 256 targets
root on rd0a swap on rd0b dump on rd0b
erase ^?, werase ^W, kill ^U, intr ^C, status ^T

Welcome to the OpenBSD/amd64 5.9 installation program.
(I)nstall, (U)pgrade, (A)utoinstall or (S)hell? I_
```

```
red
"Intel 82801AA AC97" rev 0x01 at pci0 dev 5 function 0 not configured
ohci0 at pci0 dev 6 function 0 "Apple Intrepid USB" rev 0x00: apic 1 int 22, ver
sion 1.0
"Intel 82371AB Power" rev 0x08 at pci0 dev 7 function 0 not configured
usb0 at ohci0: USB revision 1.0
uhub0 at usb0 "Apple OHCI root hub" rev 1.00/1.00 addr 1
isa0 at mainbus0
pckbc0 at isa0 port 0x60/5 irq 1 irq 12
pckbd0 at pckbc0 (kbd slot)
wskbd0 at pckbd0: console keyboard, using wsdisplay1
softraid0 at root
scsibus1 at softraid0: 256 targets
root on rd0a swap on rd0b dump on rd0b
erase ^?, werase ^W, kill ^U, intr ^C, status ^T

Welcome to the OpenBSD/amd64 5.9 installation program.
(I)nstall, (U)pgrade, (A)utoinstall or (S)hell? I
At any prompt except password prompts you can escape to a shell by
typing '!'. Default answers are shown in []'s and are selected by
pressing RETURN.  You can exit this program at any time by pressing
Control-C, but this can leave your system in an inconsistent state.

Choose your keyboard layout ('?' or 'L' for list) [default]
System hostname? (short form, e.g. 'foo') PooFlinger2000_
```

```
typing '!'. Default answers are shown in []'s and are selected by
pressing RETURN.  You can exit this program at any time by pressing
Control-C, but this can leave your system in an inconsistent state.

Choose your keyboard layout ('?' or 'L' for list) [default]
System hostname? (short form, e.g. 'foo') PooFlinger2000

Available network interfaces are: em0 vlan0.
Which network interface do you wish to configure? (or 'done') [em0]
IPv4 address for em0? (or 'dhcp' or 'none') [dhcp]
DHCPDISCOVER on em0 - interval 1
DHCPOFFER from 10.0.2.2 (52:54:00:12:35:02)
DHCPREQUEST on em0 to 255.255.255.255
DHCPACK from 10.0.2.2 (52:54:00:12:35:02)
bound to 10.0.2.15 -- renewal in 43200 seconds.
IPv6 address for em0? (or 'rtsol' or 'none') [none]
Available network interfaces are: em0 vlan0.
Which network interface do you wish to configure? (or 'done') [done]
Using DNS domainname hsd1.ut.comcast.net.
Using DNS nameservers at 8.8.8.8 4.2.2.2

Password for root account? (will not echo)
Password for root account? (again)
Start sshd(8) by default? [yes]
Do you expect to run the X Window System? [yes] no_
```

```
pressing RETURN.  You can exit this program at any time by pressing
Control-C, but this can leave your system in an inconsistent state.

Choose your keyboard layout ('?' or 'L' for list) [default]
System hostname? (short form, e.g. 'foo') PooFlinger2000

Available network interfaces are: em0 vlan0.
Which network interface do you wish to configure? (or 'done') [em0]
IPv4 address for em0? (or 'dhcp' or 'none') [dhcp]
DHCPDISCOVER on em0 - interval 1
DHCPOFFER from 10.0.2.2 (52:54:00:12:35:02)
DHCPREQUEST on em0 to 255.255.255.255
DHCPACK from 10.0.2.2 (52:54:00:12:35:02)
bound to 10.0.2.15 -- renewal in 43200 seconds.
IPv6 address for em0? (or 'rtsol' or 'none') [none]
Available network interfaces are: em0 vlan0.
Which network interface do you wish to configure? (or 'done') [done]
Using DNS domainname hsd1.ut.comcast.net.
Using DNS nameservers at 8.8.8.8 4.2.2.2

Password for root account? (will not echo)
Password for root account? (again)
Start sshd(8) by default? [yes]
Do you expect to run the X Window System? [yes] no
Setup a user? (enter a lower-case loginname, or 'no') [no] d3c4f_
```

```
, nodev, nosuid)
/dev/wd0e (f4f4856460d54158.e) on /mnt/var type ffs (rw, asynchronous, local, no
dev, nosuid)

Let's install the sets!
Location of sets? (cd0 disk http or 'done') [http]
HTTP proxy URL? (e.g. 'http://proxy:8080', or 'none') [none]
HTTP Server? (hostname, list#, 'done' or '?') [mirrors.sonic.net]
Server directory? [pub/OpenBSD/5.9/amd64]

Select sets by entering a set name, a file name pattern or 'all'. De-select
sets by prepending a '-' to the set name, file name pattern or 'all'. Selected
sets are labelled '[X]'.
    [X] bsd           [X] base59.tgz    [X] game59.tgz    [X] xfont59.tgz
    [X] bsd.rd        [X] comp59.tgz    [X] xbase59.tgz   [X] xserv59.tgz
    [ ] bsd.mp        [X] man59.tgz     [X] xshare59.tgz
Set name(s)? (or 'abort' or 'done') [done] -gam*
    [X] bsd           [X] base59.tgz    [ ] game59.tgz    [X] xfont59.tgz
    [X] bsd.rd        [X] comp59.tgz    [X] xbase59.tgz   [X] xserv59.tgz
    [ ] bsd.mp        [X] man59.tgz     [X] xshare59.tgz
Set name(s)? (or 'abort' or 'done') [done] -x*
    [X] bsd           [X] base59.tgz    [ ] game59.tgz    [ ] xfont59.tgz
    [X] bsd.rd        [X] comp59.tgz    [ ] xbase59.tgz   [ ] xserv59.tgz
    [ ] bsd.mp        [X] man59.tgz     [ ] xshare59.tgz
Set name(s)? (or 'abort' or 'done') [done] _
```

```
Set name(s)? (or 'abort' or 'done') [done]
Get/Verify SHA256.sig   100% |*****************************|  2152       00:00
Signature Verified
Get/Verify bsd          100% |*****************************| 10004 KB    00:05
Get/Verify bsd.rd       100% |*****************************|  7581 KB    00:04
Get/Verify base59.tgz   100% |*****************************| 51606 KB    00:26
Get/Verify comp59.tgz   100% |*****************************| 50520 KB    00:29
Get/Verify man59.tgz    100% |*****************************|  8779 KB    00:04
Installing bsd          100% |*****************************| 10004 KB    00:00
Installing bsd.rd       100% |*****************************|  7581 KB    00:00
Installing base59.tgz   100% |*****************************| 51606 KB    00:03
Extracting etc.tgz      100% |*****************************|   188 KB    00:00
Installing comp59.tgz   100% |*****************************| 50520 KB    00:03
Installing man59.tgz    100% |*****************************|  8779 KB    00:00
Location of sets? (cd0 disk http or 'done') [done]
Time appears wrong.  Set to 'Thu Jun 16 02:53:51 MDT 2016'? [yes]
Saving configuration files...done.
Making all device nodes...done.

CONGRATULATIONS! Your OpenBSD install has been successfully completed!
To boot the new system, enter 'reboot' at the command prompt.
When you login to your new system the first time, please read your mail
using the 'mail' command.

# _
```

```
kern.securelevel: 0 -> 1
creating runtime link editor directory cache.
preserving editor files.
starting network daemons: sshd smtpd sndiod.
Path to firmware: http://firmware.openbsd.org/firmware/5.9/
No devices found which need firmware files to be downloaded.
starting local daemons: cron.
Thu Jun 16 02:56:34 MDT 2016

OpenBSD/amd64 (PooFlinger2000.hsd1.ut.comcast.net.) (ttyC0)

login: root
Password:
OpenBSD 5.9 (GENERIC) #1761: Fri Feb 26 01:15:04 MST 2016

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

You have mail.
# _
```

Configuring the OpenBSD Operating System

- Install packages

```
# pkg_add -iv vim
quirks-2.197 signed on 2016-02-26T22:06:23Z
quirks-2.197: ok
Ambiguous: choose package for vim
a       0: <None>
        1: vim-7.4.900-gtk2
        2: vim-7.4.900-gtk2-lua
        3: vim-7.4.900-gtk2-perl-python-ruby
        4: vim-7.4.900-gtk2-perl-python3-ruby
        5: vim-7.4.900-no_x11
        6: vim-7.4.900-no_x11-lua
        7: vim-7.4.900-no_x11-perl-python-ruby
        8: vim-7.4.900-no_x11-perl-python3-ruby
        9: vim-7.4.900-no_x11-ruby
Your choice: 5_
```

```
# pkg_add -iv dnsmasq_
```

```
# pkg_add -iv vnstat_
```

Configuring the OpenBSD Operating System

- Install packages
- Kernel Module - Enable routing

```
net.inet.ip.forwarding=1
```

```
# vim /etc/sysctl.conf
```

Configuring the OpenBSD Operating System

- Install packages
- Kernel Module - Enable routing
- Setup Network Interfaces

dhcp

```
# vim /etc/hostname.em0
```

inet 10.10.10.1 255.255.255.0 10.10.10.255

vim /etc/hostname.em1

Configuring DHCP Daemon

- Make DHCPD start on boot

dhcp_flags=””

vim /etc/rc.conf.local

Configuring DHCP Daemon

- Make DHCPD start on boot
- Configure DHCPD options

```
subnet 10.10.10.0 netmask 255.255.255.0
{
        default-lease-time 604800;
        option domain-name “PooFlinger2000”;
        option domain-name-servers 4.2.2.2, 4.4.4.4;
        option routers 10.10.10.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.10.10.255;
        range 10.10.10.50 10.10.10.254;
}
```

```
# vim /etc/dhcpd.conf
```

Configuring DNSMasq

- Make DNSMasq start on boot

```
if [ -x /usr/local/sbin/dnsmasq ]; then
        echo ‘ starting: dnsmasq ‘; /usr/local/sbin/dnsmasq
fi
```

vim /etc/rc.local

Configuring DNSMasq

- Make DNSMasq start on boot
- Configure DNSMasq options

```
no-poll
no-resolv
no-hosts
server=75.75.75.75
server=8.8.8.8
cache-size=9001
local-ttl=90
auth-ttl=120
max-ttl=90
max-cache-ttl=90
log-queries
log-facility=/var/log/dnsmasq_queries.log

# LOCAL DNS REWRITES
address=/bing.com/10.10.10.5
address=/.bing.com/10.10.10.5
```

vim /etc/dnsmasq.conf

Configuring PF

- Make PF start on boot
  - (It already does!)

Configuring PF

- Make PF start on boot
  - (It already does!)
- Configure PF

```
set limit states 1000000 # one million states! Bwahahaha
set skip on lo0 # skip processing on loopback device

match out on em0 inet from em1:network nat-to (em0) # enable NAT
block quick inet6 # kill all IPv6 traffic. Dead. Bam.
block all # default block rule. no “quick” so last matching rule wins
pass from { self, em1:network }

# rewrite DNS requests to local DNSMasq Service
pass in quick on em1 proto udp from any to port 53 \
        rdr-to 127.0.0.1 tag dns

pass inet proto icmp icmp-type echoreq # allow ping requests

# Allow external->internal SSH from tcp port 2222, translated to tcp port 22
pass in on egress inet proto tcp from any to (egress) port 2222 \
        rdr-to 10.10.10.5 port 22
```

```
# vim /etc/pf.conf
```

Monitoring your new firewall / router

- CPU / Memory Utilization
  - TOP
  - HTOP

Monitoring your new firewall / router

- CPU / Memory Utilization
  - TOP
  - HTOP
- Network
  - IFTOP
  - NLOAD
  - VNSTAT
- System stats
  - Collectd / Grafana

```
# vnstat -u -i em0
Error: Unable to read database "/var/db/vnstat/em0": No such file or directory
Info: -> A new database has been created.
# vnstat -u -i em1
Error: Unable to read database "/var/db/vnstat/em1": No such file or directory
Info: -> A new database has been created.
# chown _vnstat /var/db/vnstat/*
# _
```

```
dhcpd_flags=””
pkg_scripts=”vnstatd”
```

vim /etc/rc.conf.local

```
Database updated: Wed Jun 15 22:26:07 2016

   em0 since 06/15/16

          rx:  724.42 MB      tx:  17.32 MB      total:  741.74 MB

   monthly
                     rx      |     tx      |    total    |   avg. rate
     ------------------------+-------------+-------------+---------------
       Jun '16     724.42 MB |    17.32 MB |   741.74 MB |      0.59 KB/s
     ------------------------+-------------+-------------+---------------
     estimated       1.42 GB |       34 MB |     1.45 GB |

   daily
                     rx      |     tx      |    total    |   avg. rate
     ------------------------+-------------+-------------+---------------
         today     724.42 MB |    17.32 MB |   741.74 MB |      9.40 KB/s
     ------------------------+-------------+-------------+---------------
     estimated        774 MB |       18 MB |      792 MB |
# _
```

Monitoring your new firewall / router

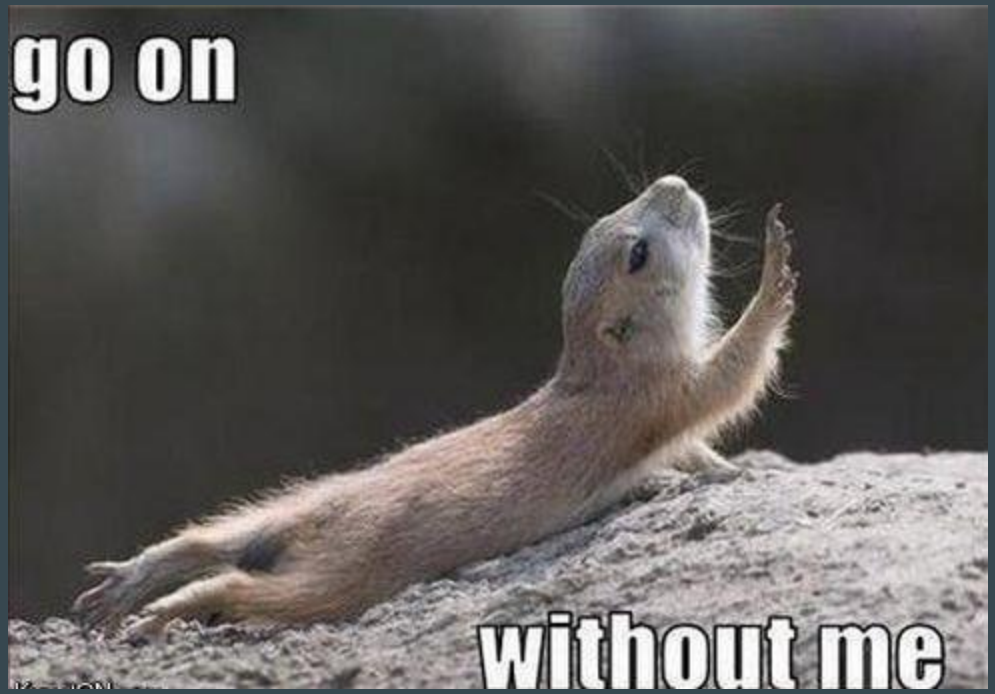
- CPU / Memory Utilization
  - TOP
  - HTOP
- Network
  - IFTOP
  - NLOAD
  - VNSTAT
- System stats
  - Collectd / Grafana
- DHCP Leases
  - tail -f /var/db/dhcpd.leases

Monitoring your new firewall / router

- CPU / Memory Utilization
  - TOP
  - HTOP
- Network
  - IFTOP
  - NLOAD
  - VNSTAT
- System stats
  - Collectd / Grafana
- DHCP Leases
  - tail -f /var/db/dhcpd.leases
- DNS Queries
  - tail -f /var/log/dnsmasq_queries.log

Monitoring your new firewall / router

- CPU / Memory Utilization
  - TOP
  - HTOP
- Network
  - IFTOP
  - NLOAD
  - VNSTAT
- System stats
  - Collectd / Grafana
- DHCP Leases
  - tail -f /var/db/dhcpd.leases
- DNS Queries
  - tail -f /var/log/dnsmasq_queries.log
- PF Information
  - pfctl -ss ; pfcfl -si ; pfctl -sr


go on
without me

Future updates to consider

- QoS (Quality of Service)
  - SUPER easy to implement via PF

Future updates to consider

- QoS (Quality of Service)
  - SUPER easy to implement via PF
- IDS / IPS / “NextGen Firewall” options
  - SNORT / OpenAppID
  - Suricata

Future updates to consider

- QoS (Quality of Service)
  - SUPER easy to implement via PF
- IDS / IPS / “NextGen Firewall” options
  - SNORT / OpenAppID
  - Suricata
- Redundancy / Failover
  - CARP / PFSync

Future updates to consider

- QoS (Quality of Service)
  - SUPER easy to implement via PF
- IDS / IPS / “NextGen Firewall” options
  - SNORT / OpenAppID
  - Suricata
- Redundancy / Failover
  - CARP / PFSync
- ...and whatever else you can think of.

Thanks for coming!

...

Please ask any questions now, before we escape!