Home Router/Firewall using OPNsense

My totally overkill home network

Shankar Viswanathan           Dec 2022
Outline

● Motivation for new home network
● SW & HW choices
● OPNsense basics
● Router & Network setup
● Power/performance
● Demo
What I had ...

- Typical consumer router running OpenWRT in the basement
- Coax between basement and first floor – MoCa adapter at each end
- First floor MoCa adapter had built-in Wifi AP
  - And Blinkenlights
It worked, but ...

- Wifi performance was poor in some rooms
  - Chicken wire in a few walls
- Latency was bad with multiple video calls in parallel
- Could never saturate 400/20 Mbps connection from ISP (over WiFi)
So ...

- Cat6A cabling installed
- 10Gbps capable over distances < 100m
But what router?

1. Standard consumer router with OpenWRT

Or

2. DIY with a router-focused OS
Winner – option #2

- Less hassle – don’t need to deal with vendor locking firmware
- No weirdness with flash size or revision number within router model
- More flexibility overall
Router OS Criteria

- Secure
- Stable
- Regular updates
- Flexible, ease of use
- FLOSS w/ reasonably active community
OS feature requirements

- Full featured stateful firewall
- DHCP server
- VLAN support
- Wireguard VPN support
- Optional: DNS filtering/blacklisting
- Optional: Traffic shaping / QoS
OS choices

- PFsense
- OPNsense
- OpenWRT
- IPFire
- Untangle
OPNsense

- Based on FreeBSD
- Fork of Pfsense
  - Itself a fork of m0n0wall
- Founded and since maintained by Deciso A.B.
- Continuously updated since its start in 2015 – 2 major updates each year
- Easy to use UI
- Fantastic documentation
## OPNsense: Major features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful Firewall</td>
<td>✔</td>
</tr>
<tr>
<td>DNS and DHCP servers, dynamic DNS</td>
<td>✔</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>✔</td>
</tr>
<tr>
<td>802.1Q VLAN support</td>
<td>✔</td>
</tr>
<tr>
<td>Link Aggregation &amp; Failover</td>
<td>✔</td>
</tr>
<tr>
<td>Traffic Shaping</td>
<td>✔</td>
</tr>
<tr>
<td>Built-in reporting and monitoring tools</td>
<td>✔</td>
</tr>
<tr>
<td>Intrusion Detection &amp; Prevention</td>
<td>✔</td>
</tr>
<tr>
<td>Virus scanner</td>
<td>✔</td>
</tr>
<tr>
<td>VPN Services (IPsec, OpenVPN, WireGuard)</td>
<td>✔</td>
</tr>
<tr>
<td>Support for plugins</td>
<td>✔</td>
</tr>
</tbody>
</table>
OPNsense installation

- Install images available for amd64 architecture only
- Can be installed from USB or flash with a display or via serial
- As with FreeBSD, finding drivers can be tricky for certain devices – Intel NICs are generally the best supported
- A “nano” image is available for embedded devices: all writes go to ramdisk, logs do not persist upon reboots
- ZFS is the recommended filesystem for standard installs
- Can install on baremetal or in a VM (VMWare, Xen, KVM etc)
- After installation, configuration can be done via console, web GUI or via ssh (ssh disabled by default)
Recommended HW

- > 1.5GHz multi-core CPU
- 4GB RAM
- Serial console or video (VGA) for installation
- > 120GB storage for OS & logs
- >= 2 NIC ports
  - Single NIC workable with a VLAN capable switch, so called “Router on a stick”
First idea

- Get a PC Engines APU2 board + enclosure kit
- Load OPNsense
- Estimated cost: ~$225
- Unobtanium :-(
Another option

- Various low power router boxes from Amazon, Aliexpress
- Deciso, Netgate, Protectli, Qotom, etc.
- 4 to 6 GbE ports
- Some come with PFSense/OPNSense preloaded
- Power draw: 15 to 35W
- Price range: $300 to $700

Image credit: qotom.com
Go down r/OPNsense rabbit hole ...

- Used slim PC or thin client with open PCIe slot
- Add 4-port GbE NIC
- Add larger disk or use USB storage
- Power: ~30W
- Estimated cost: ~$200
Get crazy deep into r/homelab

Why not get a rackmount server with a bunch of ethernet ports?
Found this on Ebay: Kemp LM3400
8GbE ports, 2 USB2, Cisco-style serial
VGA, 2 more USB2s, power
4-core SandyBridge Xeon, 8GB DDR3
And I paid ...

$53.11

(incl. tax & shipping, sans disk)
Setup

- OPNsense installed without a hitch
- All 8 GbE ports got recognized (em0 – em7)
- Configured WAN, link aggregated 2 ports to main switch for LAN
- Setup VLANs and mapped to Wifi SSIDs:
  - Internal (NAS, desktop)
  - Devices (phones, printer, streaming devices)
  - Guest
- Configured Wireguard for remote access
Network topology

- Two links between router and switch form a LAN LAG
- VLANs go over the LAG
- Managed switch has PoE+ ports to power WiFi APs
- One ceiling-mounted AP in each floor, staggered placement
As a project wears on, standards for success slip lower and lower.

0 hours
Okay, I should be able to dual-boot bed soon.

6 hours
I'll be happy if I can get the system working like it was when I started.

10 hours
Well, the desktops are lost cause, but I think I can fix the problems the laptops developed.

24 hours
If we're lucky, the sharks will stay away until we reach shallow water.

If we make it back alive, you're never upgrading anything again.
Performance: iperf3 simultaneous

Connecting to host 172.16.2.25, port 52201

[ 5] local 172.16.3.18 port 47572 connected to 172.16.2.25 port 52201

<table>
<thead>
<tr>
<th>ID</th>
<th>Interval</th>
<th>Transfer</th>
<th>Bitrate</th>
<th>Retr</th>
<th>Cwnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.00-1.00 sec</td>
<td>112 MBytes</td>
<td>940 Mbits/sec</td>
<td>0</td>
<td>744 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>1.00-2.00 sec</td>
<td>110 MBytes</td>
<td>923 Mbits/sec</td>
<td>0</td>
<td>782 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>2.00-3.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>822 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>3.00-4.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>822 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>4.00-5.00 sec</td>
<td>110 MBytes</td>
<td>923 Mbits/sec</td>
<td>2</td>
<td>605 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>5.00-6.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>723 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>6.00-7.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>758 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>7.00-8.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>758 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>8.00-9.00 sec</td>
<td>110 MBytes</td>
<td>923 Mbits/sec</td>
<td>0</td>
<td>819 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>9.00-10.00 sec</td>
<td>112 MBytes</td>
<td>944 Mbits/sec</td>
<td>0</td>
<td>834 KBytes</td>
</tr>
</tbody>
</table>

---

Connecting to host 172.16.3.18, port 5201

[ 5] local 172.16.2.25 port 54792 connected to 172.16.3.18 port 5201

<table>
<thead>
<tr>
<th>ID</th>
<th>Interval</th>
<th>Transfer</th>
<th>Bitrate</th>
<th>Retr</th>
<th>Cwnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.00-1.00 sec</td>
<td>113 MBytes</td>
<td>949 Mbits/sec</td>
<td>0</td>
<td>430 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>1.00-2.00 sec</td>
<td>112 MBytes</td>
<td>940 Mbits/sec</td>
<td>0</td>
<td>648 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>2.00-3.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>717 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>3.00-4.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>717 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>4.00-5.00 sec</td>
<td>111 MBytes</td>
<td>932 Mbits/sec</td>
<td>0</td>
<td>749 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>5.00-6.00 sec</td>
<td>110 MBytes</td>
<td>924 Mbits/sec</td>
<td>0</td>
<td>785 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>6.00-7.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>830 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>7.00-8.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>830 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>8.00-9.00 sec</td>
<td>111 MBytes</td>
<td>933 Mbits/sec</td>
<td>0</td>
<td>830 KBytes</td>
</tr>
<tr>
<td>5</td>
<td>9.00-10.00 sec</td>
<td>110 MBytes</td>
<td>923 Mbits/sec</td>
<td>0</td>
<td>830 KBytes</td>
</tr>
</tbody>
</table>

---

[ 5] 0.00-10.00 sec 1.08 GBytes 932 Mbits/sec 2 sender
[ 5] 0.00-10.01 sec 1.08 GBytes 929 Mbits/sec receiver

---

[ 5] 0.00-10.00 sec 1.09 GBytes 933 Mbits/sec 0 sender
[ 5] 0.00-10.00 sec 1.09 GBytes 931 Mbits/sec receiver

BLU, Dec 2022
Speedtest: Wired & WiFi

Wired

Download: 429.20 Mbps
Upload: 23.93 Mbps
Ping: 12 ms

WiFi

Download: 397.95 Mbps
Upload: 23.36 Mbps
Ping: 33 ms

WiFi test done in same room as AP

BLU, Dec 2022
Power

• Measurements using Kill-a-Watt showed modem+router+switch consuming 89W on average over a 48 hour period
  - Includes PoE supplied to the 2 APs
• Router alone averaged ~65W
• With some tweaks to CPU power management settings in OPNsense, total average power came down to 77W
  - Fixed CPU frequency to 1600MHz (was adaptive earlier)
  - Enabled CPUs to go down to ACPI C3 state

```plaintext
dev.cpu.0.freq_levels: 3101/95000 3100/95000 3000/90163 2900/86347 2800/82600 2700/78924 2600/74419 2500/70905 2300/64048 2200/59864 2100/56612 2000/53437 1900/50315 1800/47257 1700/43458 1600/40536

dev.cpu.0.freq: 1600

dev.cpu.0.cx_supported: C1/1/1 C2/2/80 C3/3/104

dev.cpu.0.cx_lowest: C3
```
Demo time