

Homelab Escapades

Newcastle Cybersecurity Group

Jay Rovacsek

February 23, 2021

Public speaking skills: a solid 2.5/10 - remind me now that I
should slow down and chill-out

If you have questions at any point feel free to jump in!



\$whoami: I work for nib as part
of the cybersecurity function



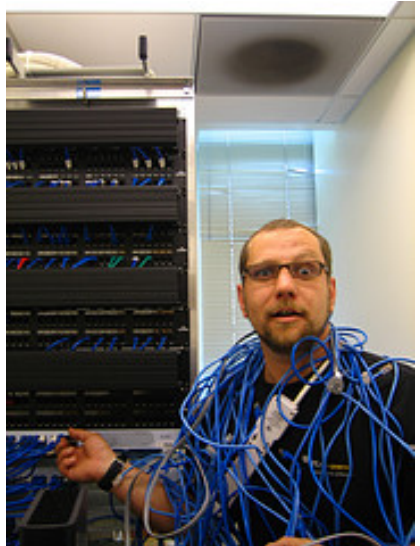
Previous lives as:

- developer
- retail assistant
- pizza cutter
- lawn mower



What am I not?

- A sysadmin
- Good at making presentation slides



Does any of this matter?

Just keep in mind, I'm just some
dude throwing some things
together and hoping for the best

Nope



But why am I here presenting?

~_(\ツ)_/-

- Home networks are fun
- Breaking your own stuff will assist in teaching you
- Can run some cool services for yourself/family/friends

Who is currently running their own hobby networks?

What are you currently running?

Am I going to be making any assumptions?

- We're not wanting to have a large number of physical devices
- We care about the security of our stuff

Are there reasons to not run a service on your home network?



What might we do to a home network to not secure it?

- Disparate, inconsistent, or no authentication on services
- Failure to segment devices based on use-case or trust of the devices
- Not implement any basic IPS/IDS
- Not ensure egress traffic utilising insecure protocols are managed suitably (DNSSEC, DoH or DoTLS enforcement)
- No analysis of traffic patterns

What services might we want to run?



Should we expose these services?



I want to be able to access my
services from anywhere!



Cheatsheet for building a home network:

- 1 Buy a domain, or use a freebie
- 2 Pester your ISP for a static address (or big-brain it with some dynamic DNS)
- 3 Setup some port forwards
- 4 ????
- 5 Profit!

fin

Okay, cool, I have the things available on the interwebs...

Should we leaving our
applications in a default state?



Nope! Let's apply some defence
in depth!



I happen to have killed hours of my spare time implementing:

- Overkill network segmentation (sorry Sarah, I'll fix your chromecast connectivity one day)
- Complete traffic analysis via Snort
- Transparent DNS request rewrites via a DoH proxy
- Consistent authentication for my exposed services (there are limits here)

I am still looking to kill hours of my time with:

- Analysis of traffic patterns to identify potential issues (Zeek)

Is anyone currently utilising Zeek or have any insight into traffic pattern analysis?

Let's talk about free options that preserve privacy and security while imposing very little technical barrier to entry:

- Authelia (strong authentication protections on all yo' things)
- Pfsense/OPSense (or why you shouldn't accept your ISPs garbage)
- Snort (proactive blocking of script kiddies)

If we have time at the end of this talk I'd love to talk about some items that are less about homelab security and more about individual security:

- Robust approaches to backups
- Self management of secrets (getting out of the potential trap that is SaaS Password Managers)
- Implementing your own VPN

Ever looked at the dumpsterfire
that is an nginx config?

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
    worker_connections 768;
    # multi_accept on;
}

http {

    ##
    # Basic Settings
    ##

    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 65;
    types_hash_max_size 2048;
    # server_tokens off;

    # server_names_hash_bucket_size 64;
    # server_name_in_redirect off;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    ##
    # SSL Settings
    ##

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # Dropping SSLv3, ref: POODLE
    ssl_prefer_server_ciphers on;

    ##
```

I don't actually mind them, but
we'll assume that we ain't got
time for that



How to get around learning the intricacies of nginx?

Get some SWAG!







This SWAG...

<https://github.com/linuxserver/docker-swag>



Why SWAG?

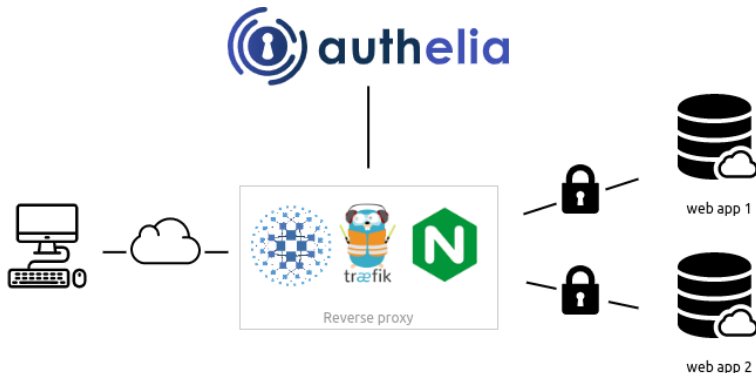
- It's a batteries included approach to us getting Authelia in the mix.
- It contains default configs for nginx come with options for Authelia included but disabled.
- Includes Let's Encrypt automation in the box

Note: **SWAG is not required, it will just make your life easier in managing a reverse proxy**

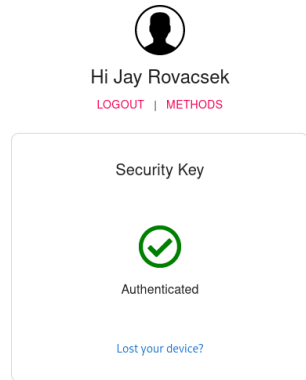
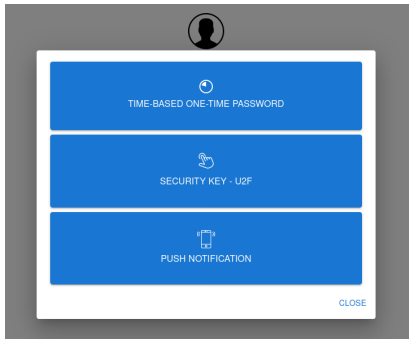
If you have the know-how of setting up a reverse proxy of your choosing, you could do so.

You could use HAProxy or Traefik instead if you're inclined

We're looking to deploy this model to our network:



So we've got SWAG and Authelia setup, what does this achieve?



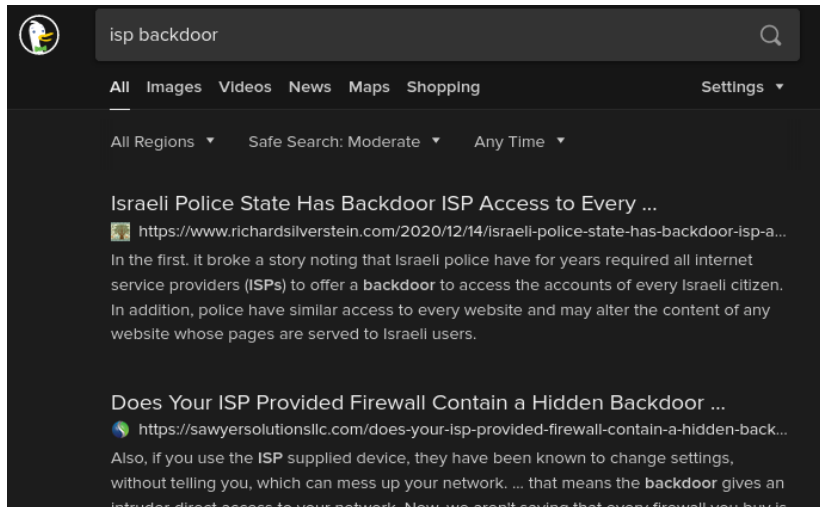
Powered by Authelia

What does the authentication flow look like? (do we chance a live demo?)

Any questions on Authelia?

On to firewall options

Why might we care to use an open-source firewall appliance over an ISP provided one?



The screenshot shows a DuckDuckGo search interface with the query "isp backdoor". The search results are displayed in a dark theme. The first result is titled "Israeli Police State Has Backdoor ISP Access to Every ..." and links to a website. The second result is titled "Does Your ISP Provided Firewall Contain a Hidden Backdoor ...".

Search Query: isp backdoor

Navigation: All Images Videos News Maps Shopping Settings

Filters: All Regions Safe Search: Moderate Any Time

Result 1:
Israeli Police State Has Backdoor ISP Access to Every ...
<https://www.richardsilverstein.com/2020/12/14/israeli-police-state-has-backdoor-isp-a...>
In the first, it broke a story noting that Israeli police have for years required all internet service providers (**ISPs**) to offer a **backdoor** to access the accounts of every Israeli citizen. In addition, police have similar access to every website and may alter the content of any website whose pages are served to Israeli users.

Result 2:
Does Your ISP Provided Firewall Contain a Hidden Backdoor ...
<https://sawyersolutionsllc.com/does-your-isp-provided-firewall-contain-a-hidden-back...>
Also, if you use the **ISP** supplied device, they have been known to change settings, without telling you, which can mess up your network. ... that means the **backdoor** gives an intruder direct access to your network. Now, we aren't saying that every firewall you buy is