Turning your home into a Cyber Fortress

Dale Land

Security Day **May 2020**

BRITISH COLUMBIA

Ministry of Citizens' Services

Your home, sometimes your office . . .

A few tips on how to improve your home cyber security.

Tuesday, June 2, 2020

Aspects of Home Cyber – think Layers

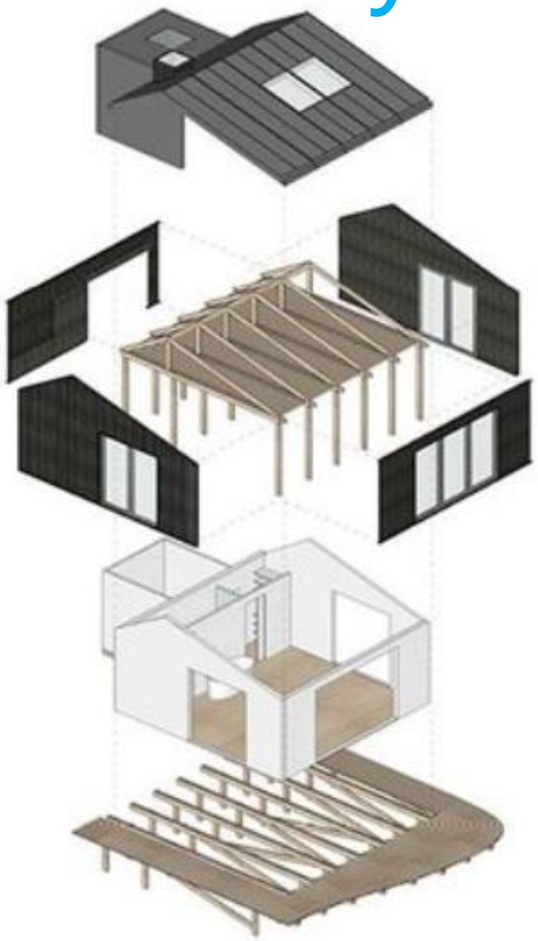
Physical

Networks

Computers

Applications

Data



Physical "The Foundation"

Tuesday, June 2, 2020

Physical Best Practices Summary

- Conduct sensitive work in a dedicated space. Limit visibility and sound transmission
- Keep your valuables safe when unattended. This includes your computer(s) and associated equipment
- Computers need a good source of power. Consider UPS if you experience interruptions. Will help prevent data loss and equipment failure
- Wired “ethernet” network is easier to protect than Wireless WiFi
- Keep any external DATA devices safely stored and protected*.

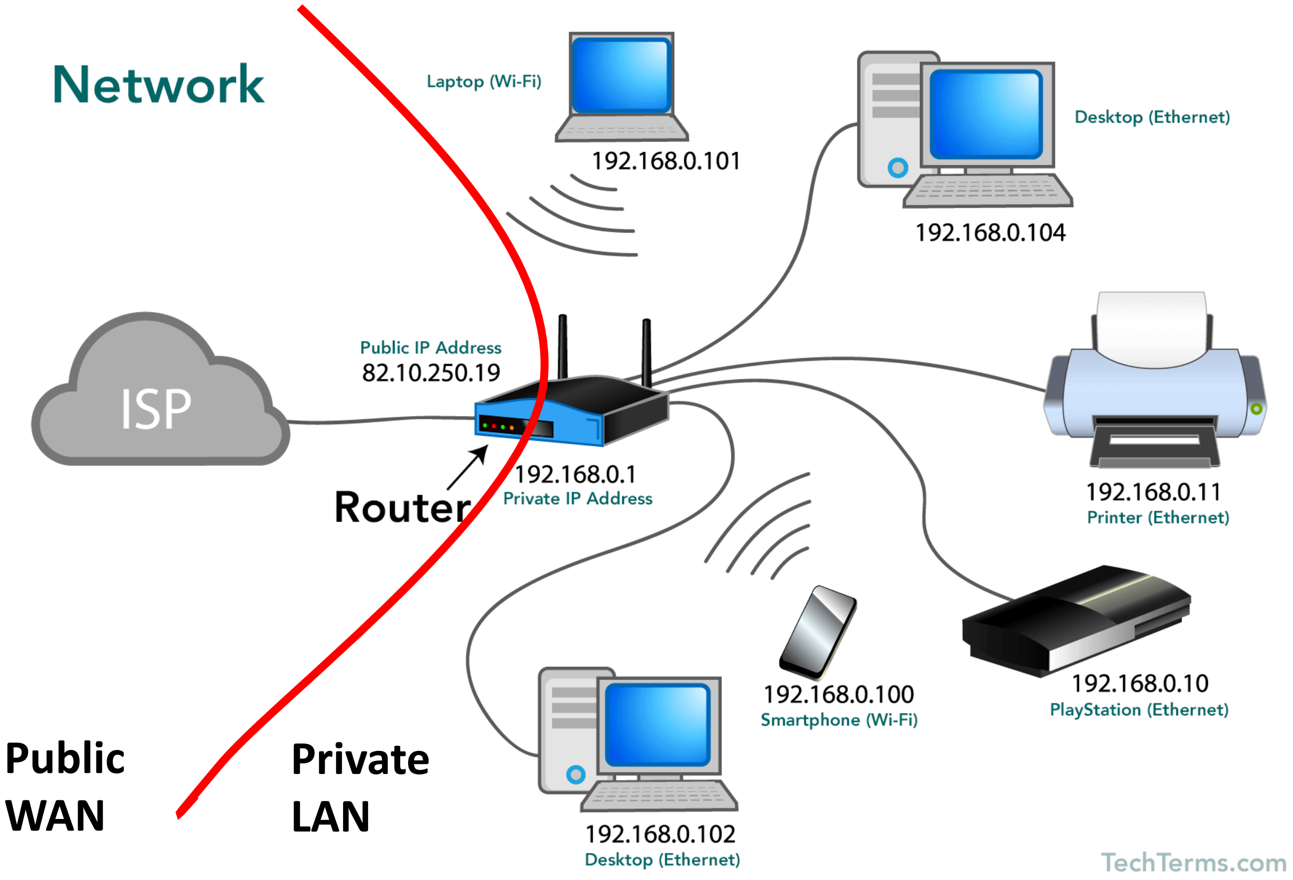
Your Cyber Threshold to the world

Let's see how it all connects

(Securely)

Home Network

Home Network Basics



Tuesday, June 2, 2020

ISP Border Considerations – Firewall & IPS

- Traffic to/from your Home <-> ISP <-> Internet
  - Inside your home is a Private Address Space (192.168.x.x or 10.x.x.x)
  - Outside your home is a “NAT” public address (64.x.x.x(T), 24.x.x.x(S)

- NAT – Network Address Translation
  - Each device on your private home network has a unique IP address.
  - Many private IP’s map to 1 Public IP (uses TCP/UDP ports to multiplex)

- Most home ISP routers come with a built in Firewall
  - *Most* home configs only need to allow outbound initiate.

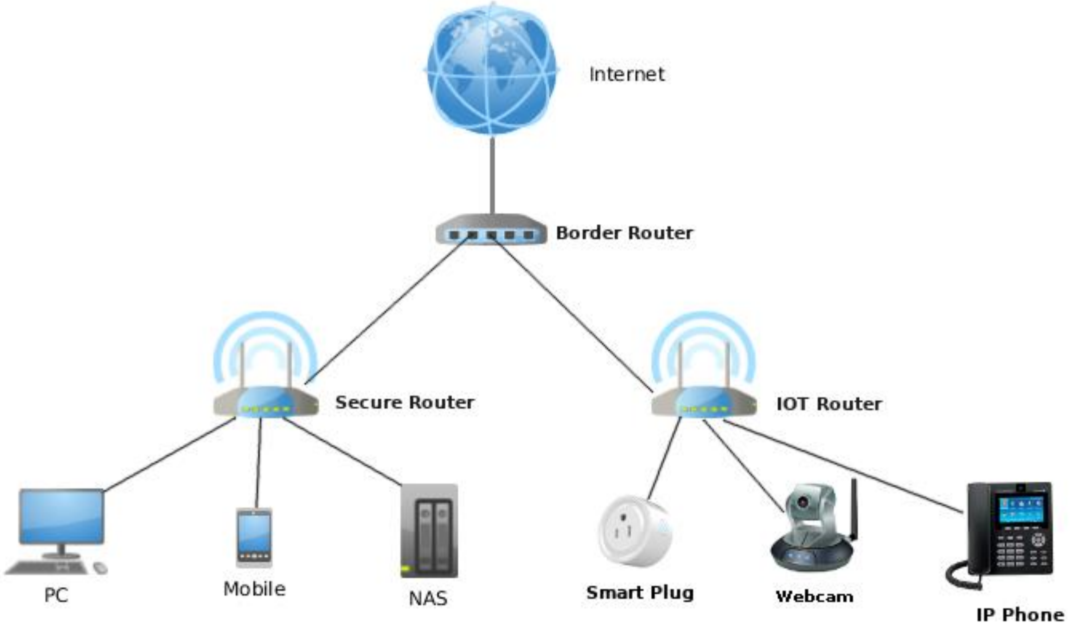
No inbound unsolicited traffic.

Adding your own home border security

- Lots of choices: May products incorporate good configurable firewall and some with intrusion protection and threat feeds for dynamic protections.
- Examples (Disclaimer – I have stock in any of these)
  - DIY: Small Linux box with IPTables or RaspberryPi with pfSense
  - Several commercial options; dedicated or part of a wireless access point/router. Netgate SG-1100 (pfSense), Synology RC2600AC, Gryphon AC3000

How to structure your home network?

OR



Tuesday, June 2, 2020

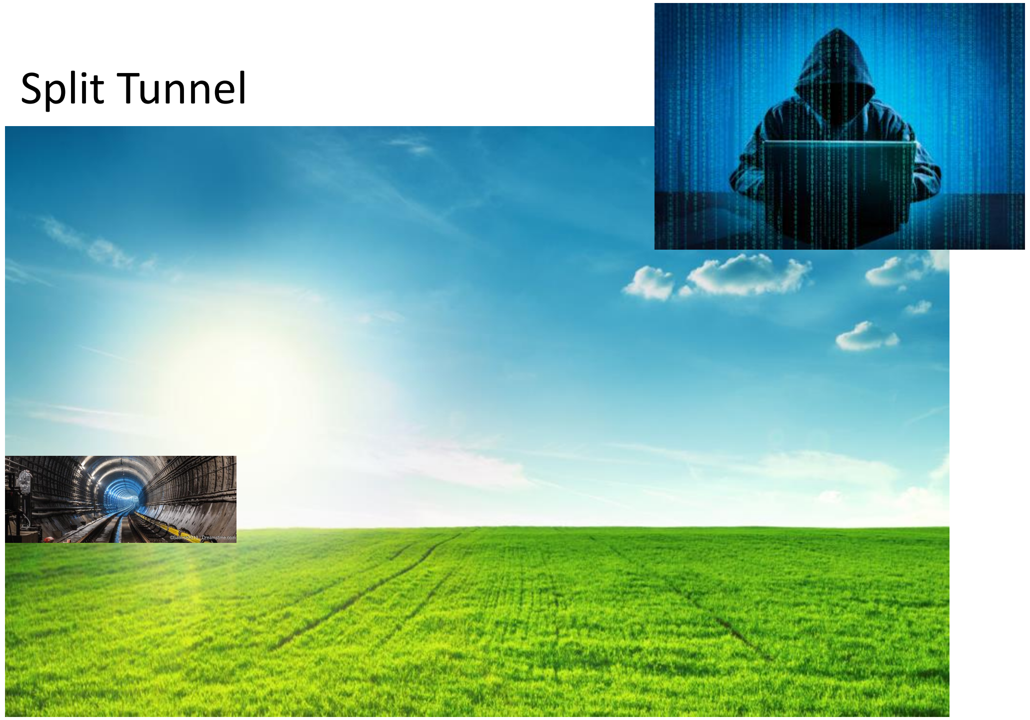
Virtual Private Networks – Why and How

Full Traffic Tunnel - IPSec or SSL

©Saoirse2010 | Dreamstime.com

vs.

Split Tunnel

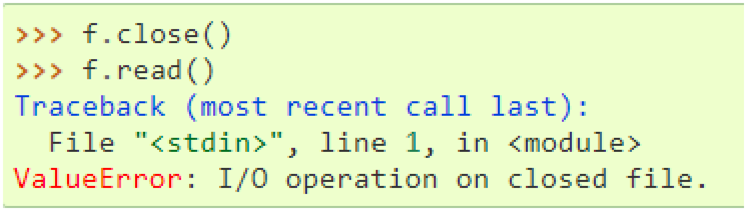


Network Best Practices Summary

- Segregate your “traditional” computers from your IOT stuff.
- Ensure your ISP Firewall is ‘On’ and disable unsolicited inbound connections. Add your own if not sure or want more control.
- If you need VPN, try and not use “split tunnel” i.e. ensure all your traffic goes through VPN – cuts off any persistent cyber criminal.

“Computers” aka network devices. . .

What are the risks



```
>>> f.close()
>>> f.read()
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
ValueError: I/O operation on closed file.
```

- Computer is a loose term in the home.
 -> Let's define it as a network component that runs code.

- Code has bugs.   Unintended functions….

- Some are patchable, and configurable. Others are not….
  - Change any default passwords on all device wherever possible

- Some offer local services,   Some reach out to the "Mother Ship"
  - Turn off remote management feature wherever possible

Computer care

- Patch, Patch, and Patch

Anti-Virus Anyone?

Anti-Malware is better - behavioral

- Segregate by function / data sensitivity where possible
  - Limit what else can talk to them

- Control how they communicate
  - Limit the "services" they offer
  - Limit who they can connect out to…

Computer Best Practices

- Know what “computers” are on your network
- Patch the cr*p out of them
- Configure them correctly – change default passwords, Turn off all non-essential call home features.
- Configure them for “least access” if possible.

Data

- Data in house or in cloud?
- Data Sensitivity? Public or Private?

ComputerHope.com

On Premise Data

- Where is your local data stored?
- How do you protect the Private data?
- Backups -> Any data that is not backed up is by definition disposable…
- Keep a backup copy off-line. i.e. not on the computer or network.

In the “Cloud”

- Encrypt your private data.
  - Lots of free tools out there.
  - Big cloud services like Azure, AWS have good tools

- Protect and don’t loose your private keys!
  - No key – no data

Data Summary

- Keep it safe, encrypt private data

- Back it up. Keep the backups off-line
  - If in the cloud, don’t keep the access keys cached.

- Manage Need-to-Know

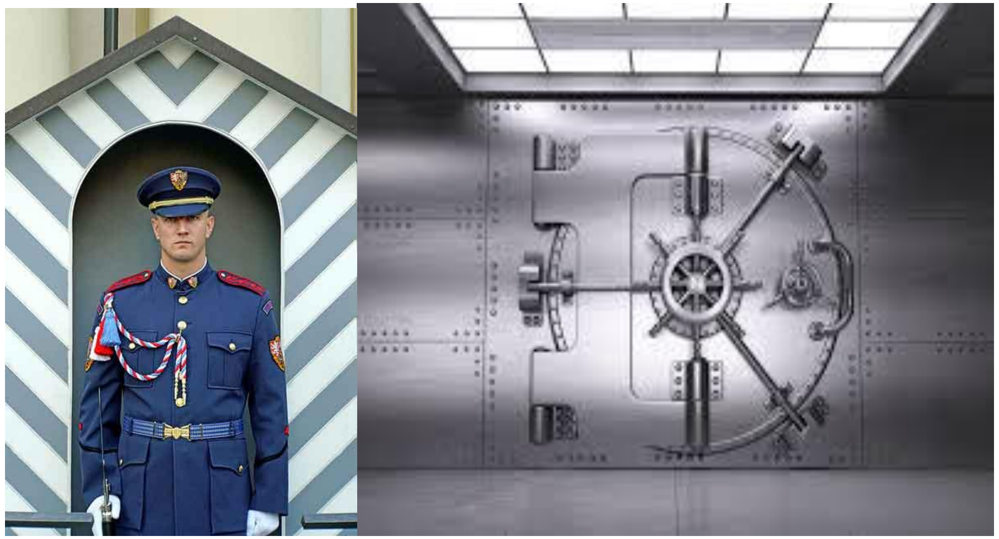
Applications

- Accessing Cloud Applications
- Accessing Work Applications
    - VPN or Not?
    - Split Tunnel or Not
- The services you offer the world
    - Intentionally or Not

Cloud Applications

TLS “Secure” web session

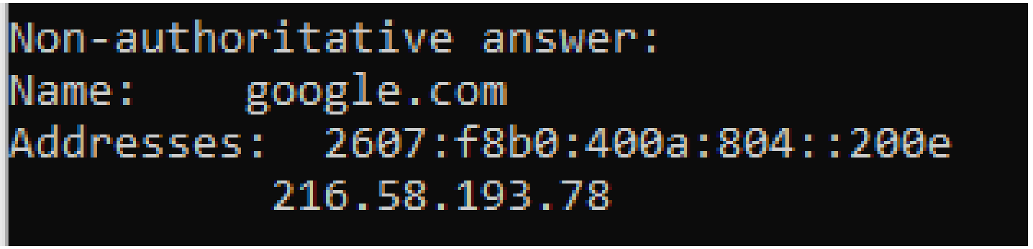
Strong Authentication



Multifactor Authentication

Quick Side Topic – “clean” DNS

- **Domain Name Service** – How a computer finds an actual destination service from a human readable name.
- i.e. google.com translates to

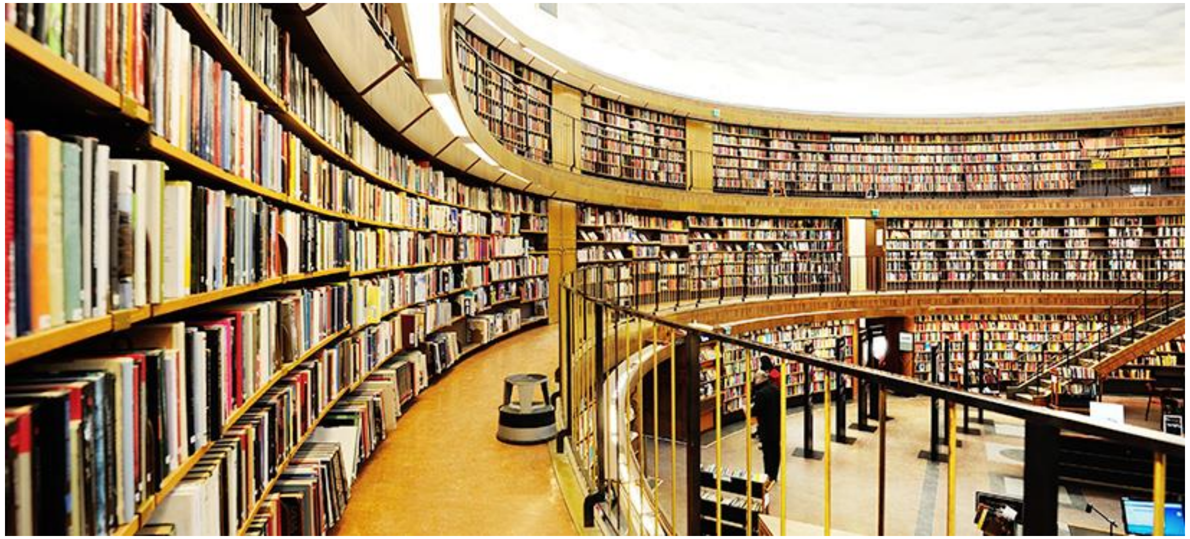


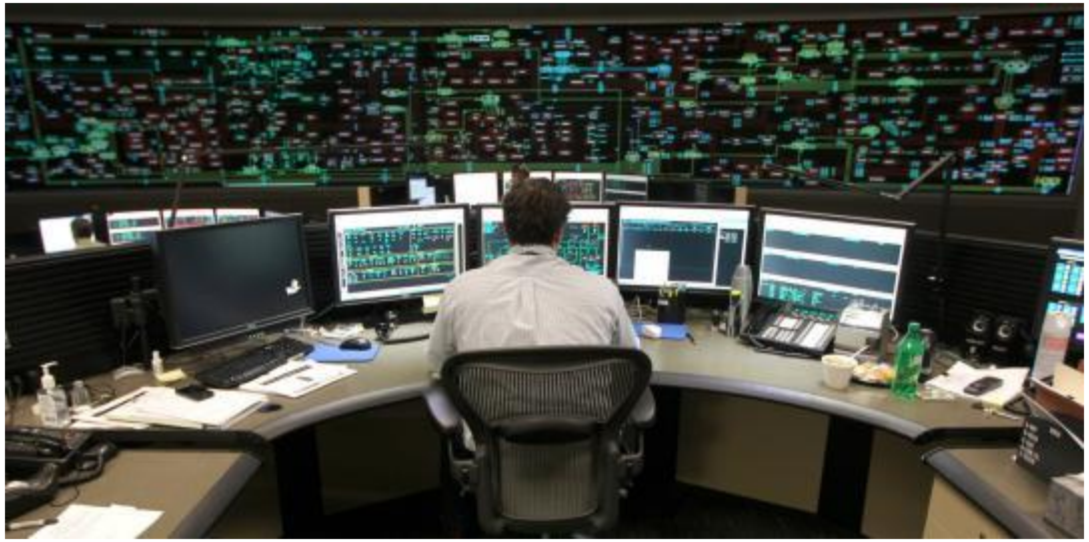
```
Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:400a:804::200e
          216.58.193.78
```

- Wouldn’t it be nice if we could clean up the unwanted ads and malicious sites?
- Google “safe dns” and do a little research.

Pi-hole®

Work Applications





Tuesday, June 2, 2020

What you offer to the World (or some)

vs.

Tuesday, June 2, 2020

Application Best Practices

- Know what you need to access and how the connection is protected
- Know all (if any) of the applications you offer the world and diligently manage them.
- Watch for potential leaking between apps due to potential application (or browser) weakness.

Final Thoughts

- Your home Cyber Fortress is like a onion, think about the layers… Each layer builds upon the previous.
- Each layer has unique characteristics and best practices
- The key is to understand how it works best together
- Keeping it secure means peace of mind….

Thank You for Listening!

Questions?