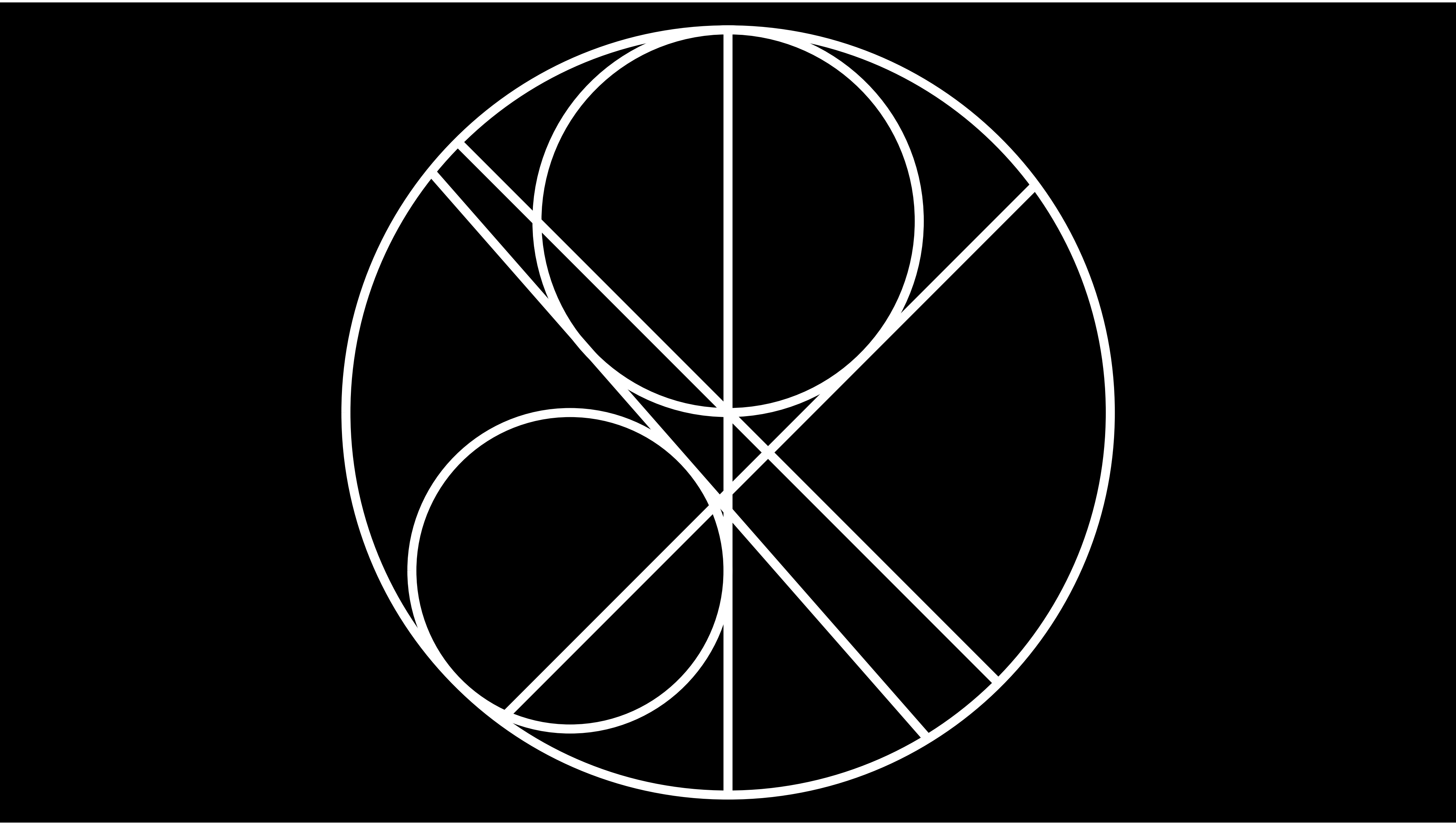


Virtual Private Networks

What are they?

Disclaimer

- All material presented is not representative of my employer or any other party
- All thoughts, ideas, and opinions are my own unless otherwise stated

Overview

- Bio
- What is a VPN
- How to choose a commercial VPN
- How to deploy your own VPN
- Summary
- Questions

Who am I?

- Jacen Kohler
- Education:
  - UNT alumni, BS in in Computer Engineering
  - SrDesign Capstone: NASA IPv6 DHCP in Space
- Career:
  - Goldman Sachs: Summer Intern & FTE Cyber Security Analyst
  - Big4 Consulting: Sr Cyber Security Consultant
  - Critical Mfg: Vulnerability Management Program Lead
- Community:
  - BSides DFW
  - Dallas Hackers Association
  - SouthWest CCDC Red Team Lead

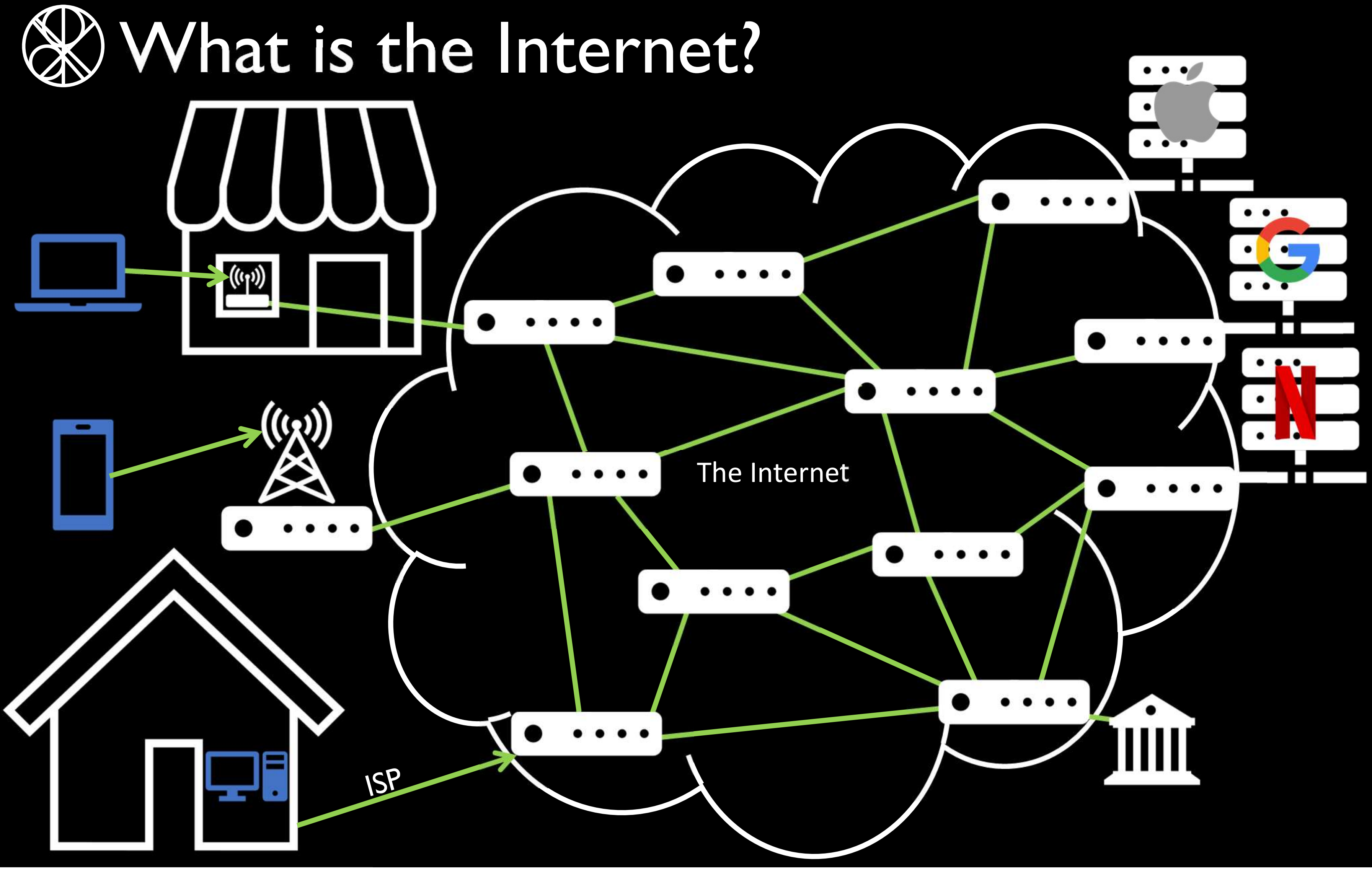
What is a VPN

- Virtual Private Network
  - “virtual point-to-point connection through the use of tunneling protocols over existing networks” – Wikipedia
  - “Allows you to access the public internet via a secure and private network connection.” – Microsoft
  - A way to access devices and networks from another network or location
  - How does a VPN work?

How Does the Internet Work?

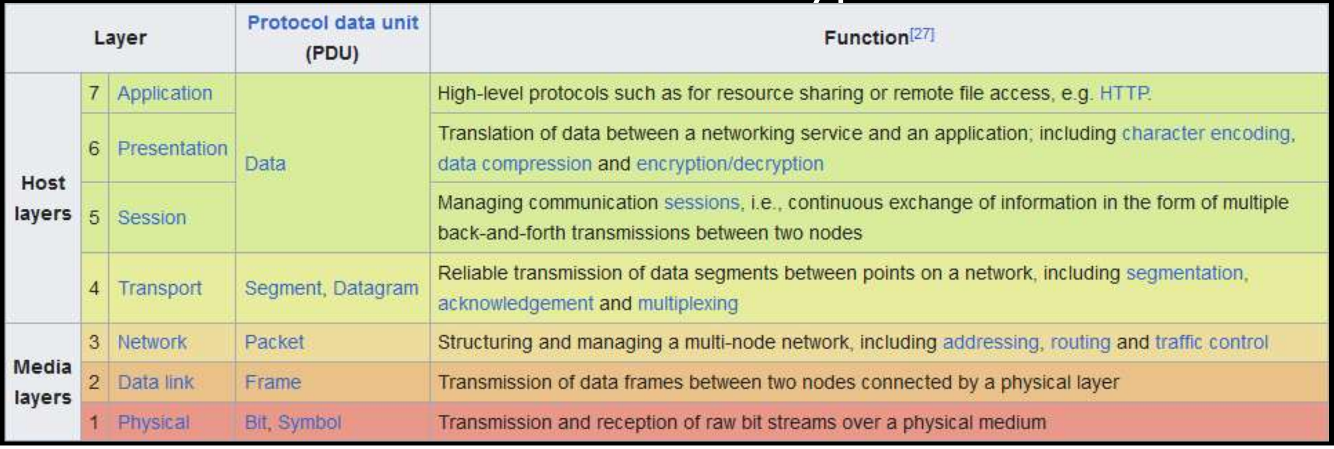
- What is the internet?
- Open Systems Interconnection model (OSI model)
- Postal example

What is the Internet?



How Does the Internet Work?

- Open Systems Interconnection model (OSI model)
  1. Physical: start and end nodes are known/detectable for a given step
  2. Data Link: start and end nodes are known/detectable for a given step
  3. Network: source and destination IP addresses are known for entire trip
  4. Transport: source and destination ports are known for entire trip
  5. Session: used for creating a single communication “conversation”
  6. Presentation: protocol conversion and data compresion
  7. Application: contains content, often encrypted via HTTPS



Layer			Protocol data unit (PDU)	Function[27]
Host layers	7	Application	Data	High-level protocols such as for resource sharing or remote file access, e.g. HTTP.
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Transmission of data frames between two nodes connected by a physical layer
	1	Physical	Bit, Symbol	Transmission and reception of raw bit streams over a physical medium

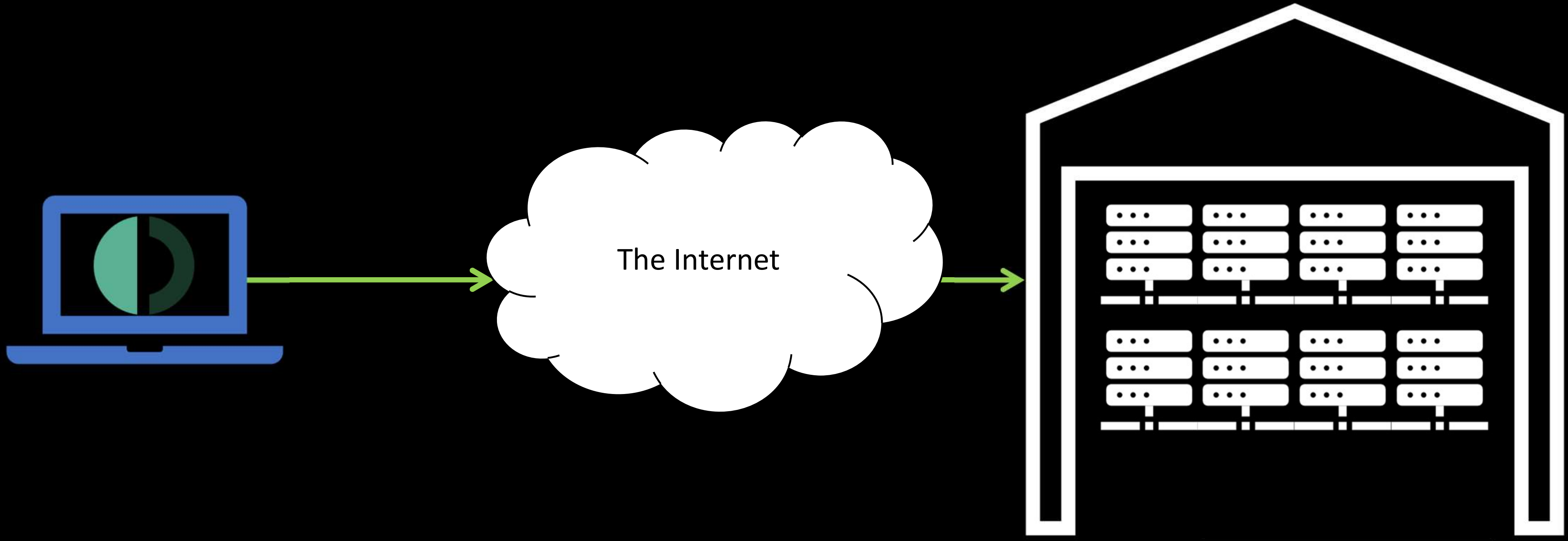
Postal Mail Example

- Open Systems Interconnection model (OSI model)
  1. Physical: Road between two USPS facilities
  2. Data Link: Address of two USPS facilities
  3. Network: Addresses for source and destination of mail
  4. Transport: Unit number for source and destination of mail
  5. Session: Similar to the stamp in that it is single use for this piece of mail
  6. Presentation: The envelope itself, can be nested in other envelopes
  7. Application: Actual contents of envelope or parcel

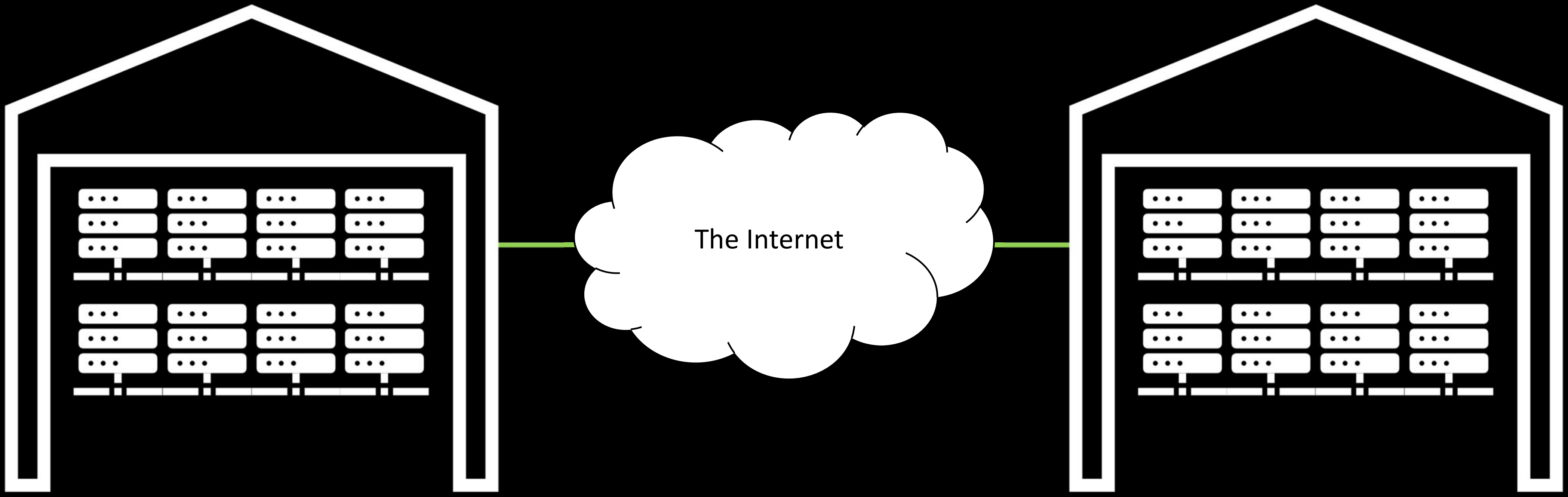
Types of VPNs

- Remote Access
- Site to Site
- Extranet
- TOR

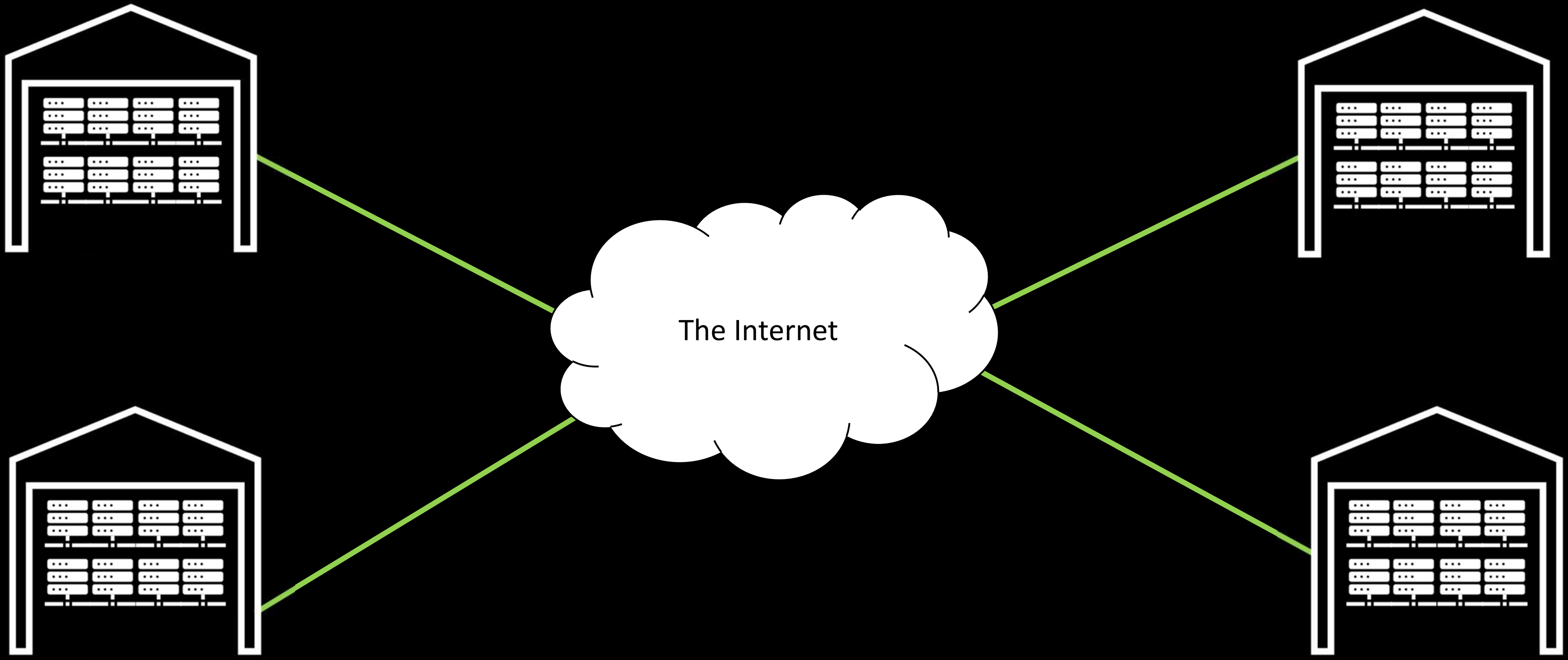
Remote Access



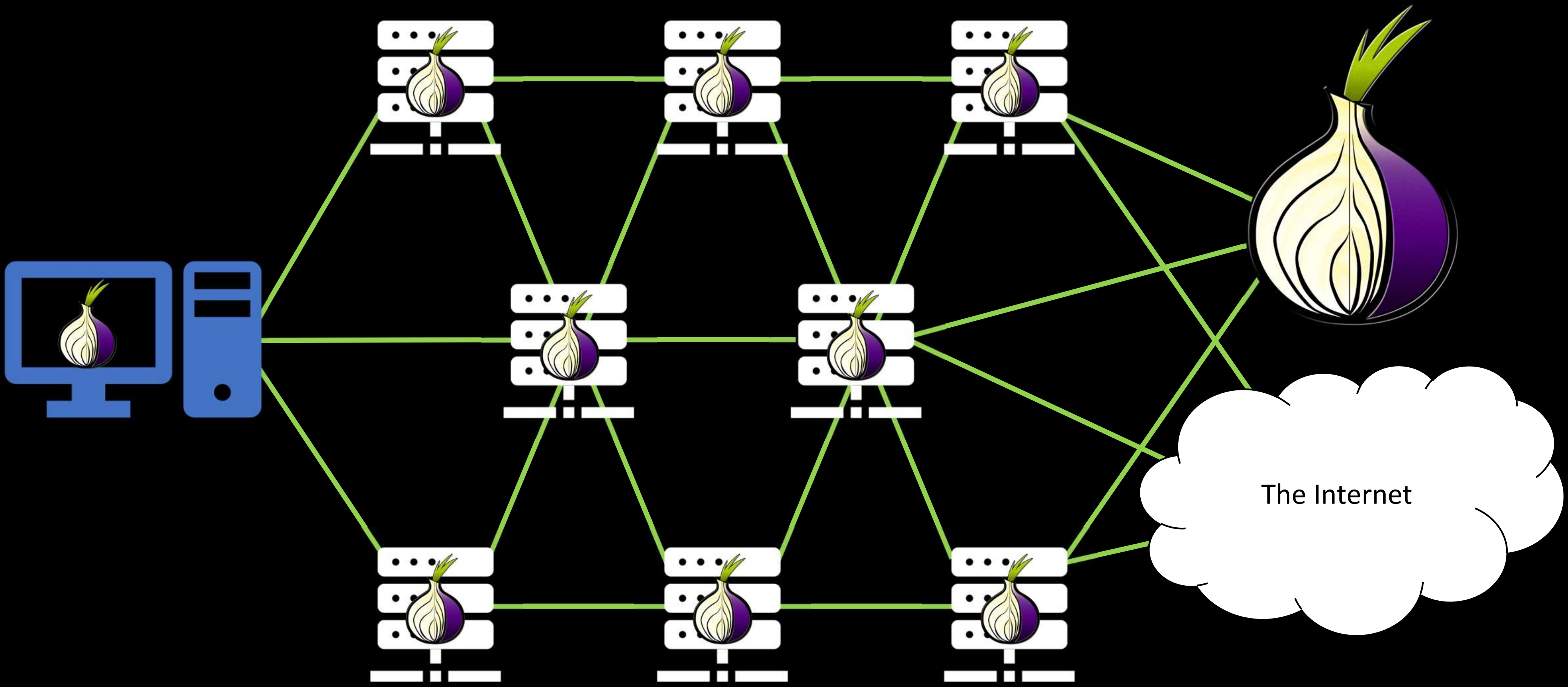
Remote Access



Extranet



TOR



What a VPN is not?

- What a VPN MIGHT be
  - Encrypted
  - Hides destination from those who can intercept traffic
- What a VPN is not?
  - SSL/TLS
  - Encrypted (potentially)

Threat Modeling

- Questions to ask yourself:
  - Why are you interested in a VPN?
    - Hide you location
    - Protect your identity
  - What are you attempting to protect yourself from?
    - Advertisers and marketers
    - Internet Service Providers (ISP) snooping
  - Who are you wanting to prevent from seeing your traffic destination?
    - ISP
    - Destination website/services
  - What other ways can these entities collect information about you?
    - Overly broad app permissions on phones
    - User submitted information

What to look for in a commercial VPN

- What jurisdiction (geography) are they located in?
  - Five Eyes: US, UK, Canada, New Zealand, Australia
  - Nine Eyes: Five Eyes, Denmark, France, the Netherlands, and Norway.
  - Fourteen Eyes: Nine Eyes, Germany, Belgium, Italy, Sweden, and Spain.
- Have they been audited?
- Do they log your traffic?
- What is their payment method?

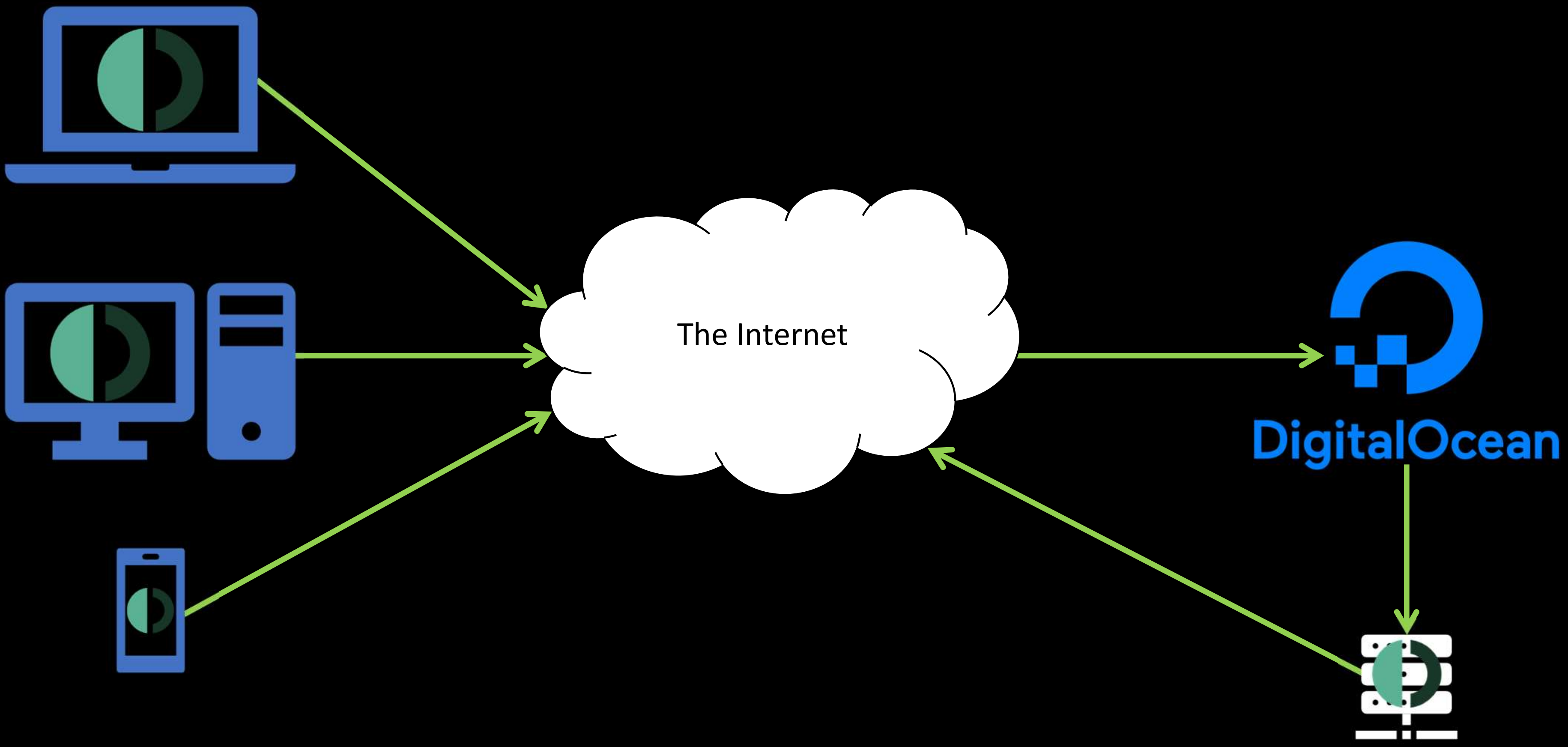
How to deploy your own VPN

- Deploy Outline to a Digital Ocean Droplet
- Deploy OpenVPN to a home router

How to deploy Outline to a Droplet

- What is Outline?
  - Simple VPN using shadowsocks
  - Part of Google's incubator Jigsaw
    - Uses technology to address geopolitical issues
    - Independently audited most recently in 2022-Dec
  - Open source
- What is Digital Ocean?
  - Cloud service provider
  - Historically friendly to hosting VPNs
- What does this method achieve?
  - Makes your traffic appear to originate from the cloud service provider
  - Does not make you invisible

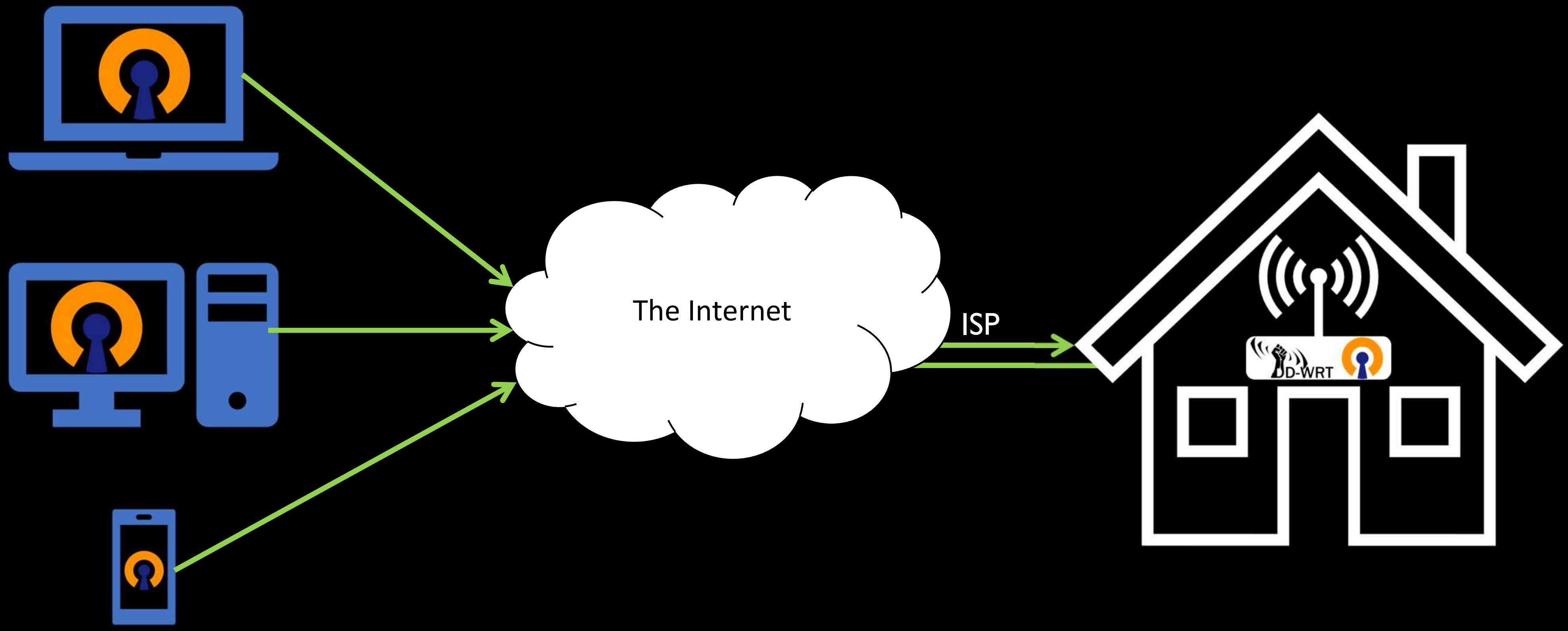
What We are Building



How to deploy OpenVPN to a Router

- What is OpenVPN?
  - Open Source VPN software using OpenSSL
- Does it need to be a router?
  - Could be a server
    - Still requires router configuration
- What does this method achieve?
  - Allows you to access devices in your home network
    - Printers
    - File servers
    - Smart Home devices

What We are Building



Summary

- Bio
- What is a VPN
- How to choose a commercial VPN
- How to deploy your own VPN
- Summary
- Questions

Questions

JacenRKohler.net

LinkedIn.com/in/JacenRKohler

@JacenRKohler

InfoSec.Exchange/@JacenRKohler

GitHub.com/JacenRKohler/Presentations