Networking & Firewalls

Cyrus Jian Bonyadi, PhD CMSC ‘21

Outline

- Background Information
    - CIA Triad
    - Preliminary Example
- Networks
    - OSI Model
    - 5 Layer Model, explained
    - Tools
- Network Security
    - Least Privilege
    - Firewalls
- Lab
    - Linux
    - Windows

Background Information

CIA Triad

Confidentiality: privacy of data

- encryption, protocols

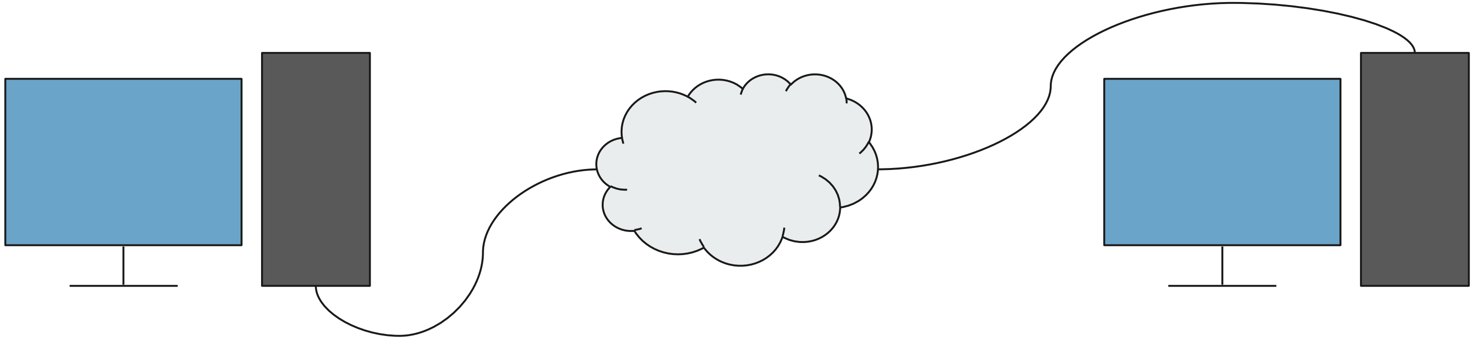
Integrity: accuracy of data

- checksums, authentication/signatures, protocols,

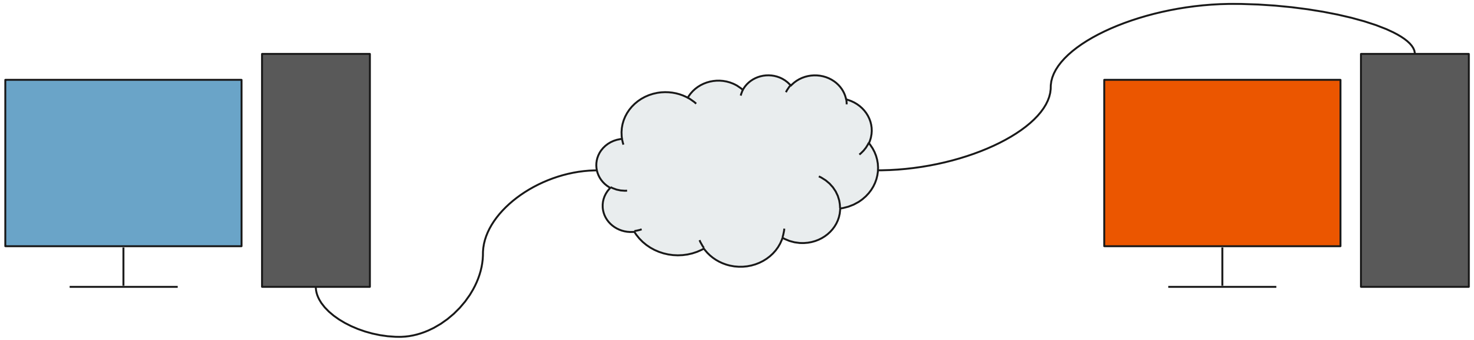
Availability: access to data

- firewalls, routing,

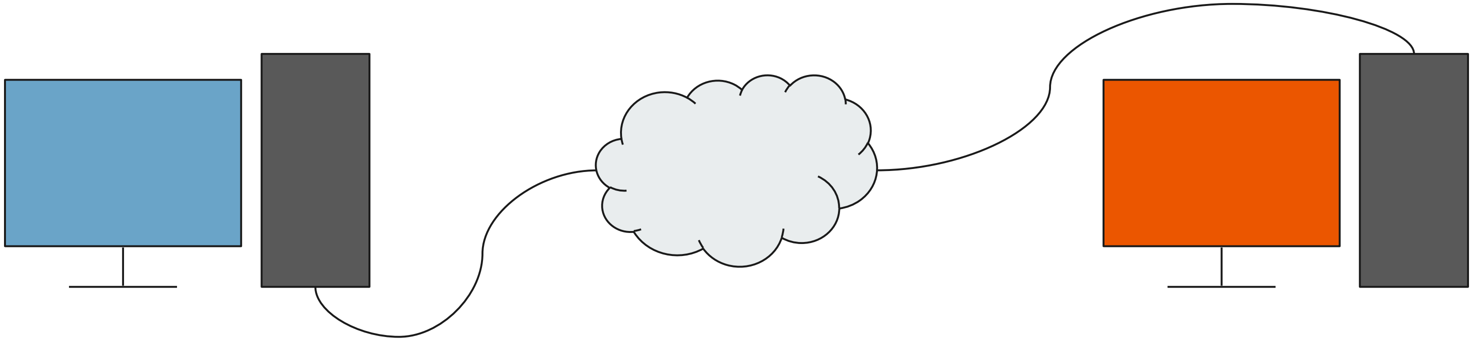
Preliminary Example



Preliminary Example

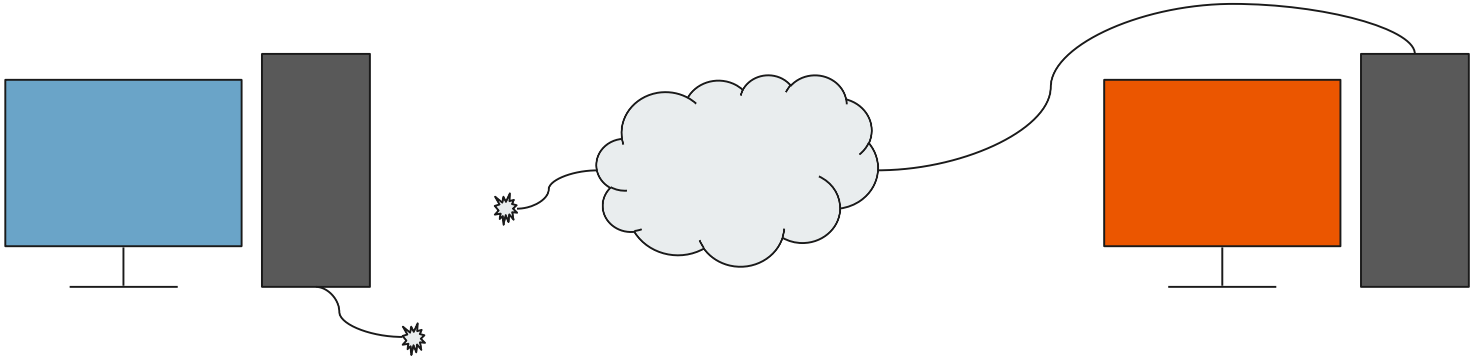


Preliminary Example

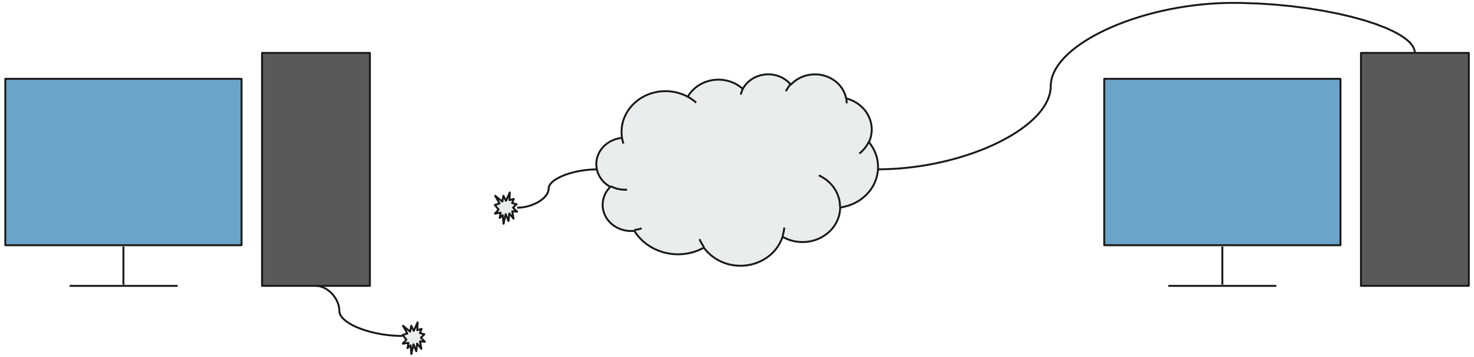


What is the easiest way to protect good users?

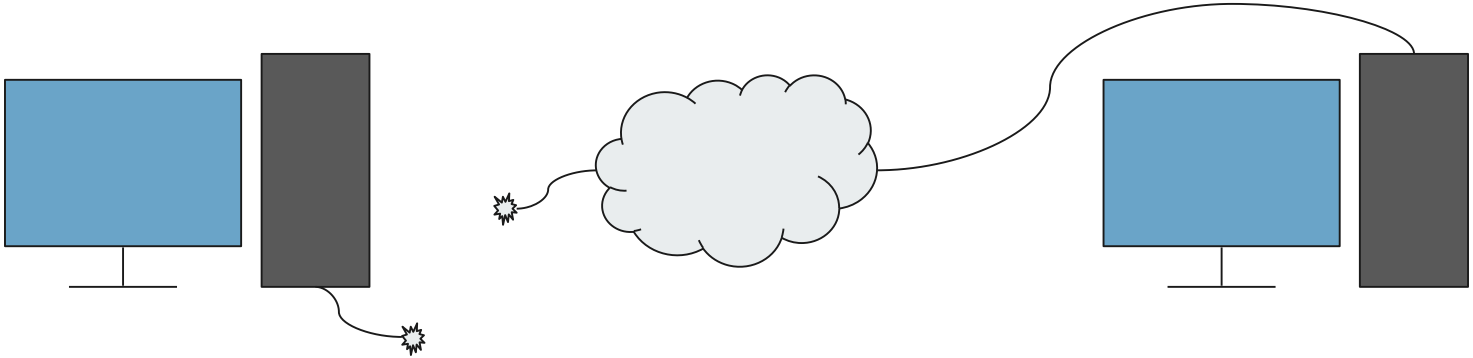
Preliminary Example



Preliminary Example



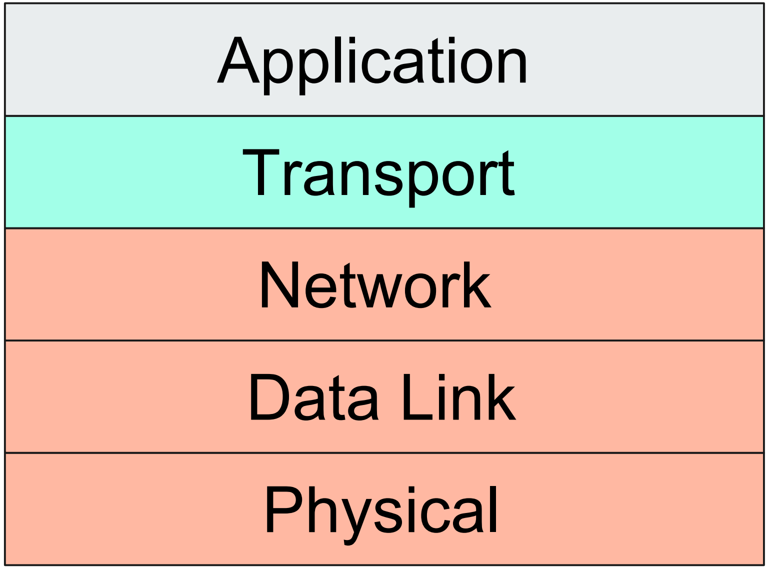
Preliminary Example



Problem: Confidentiality and Integrity without Availability

Networks

Network Fundamentals



Application

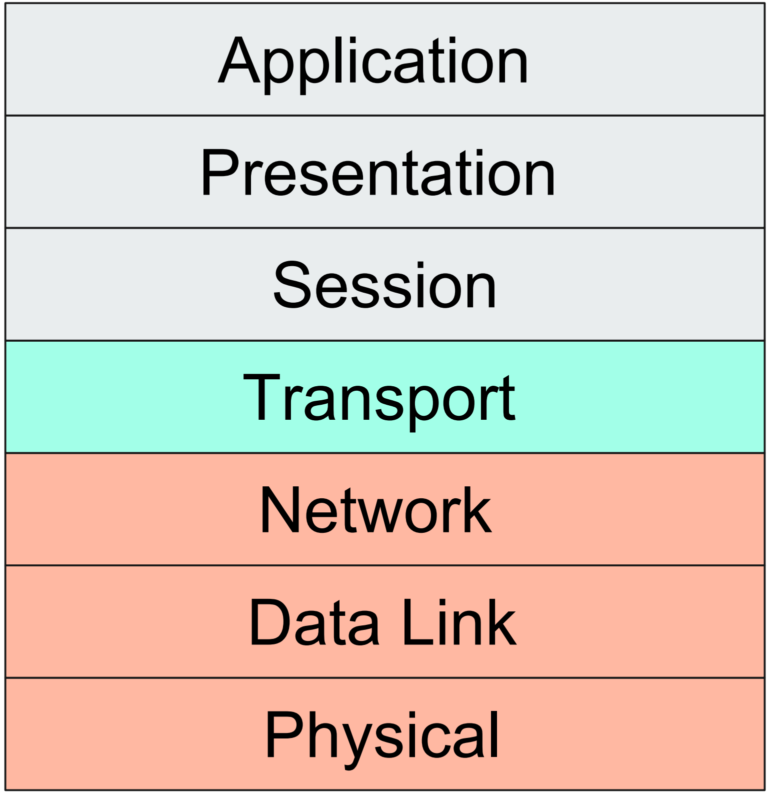
Transport

Network

Data Link

Physical

5 Layer



Application

Presentation

Session

Transport

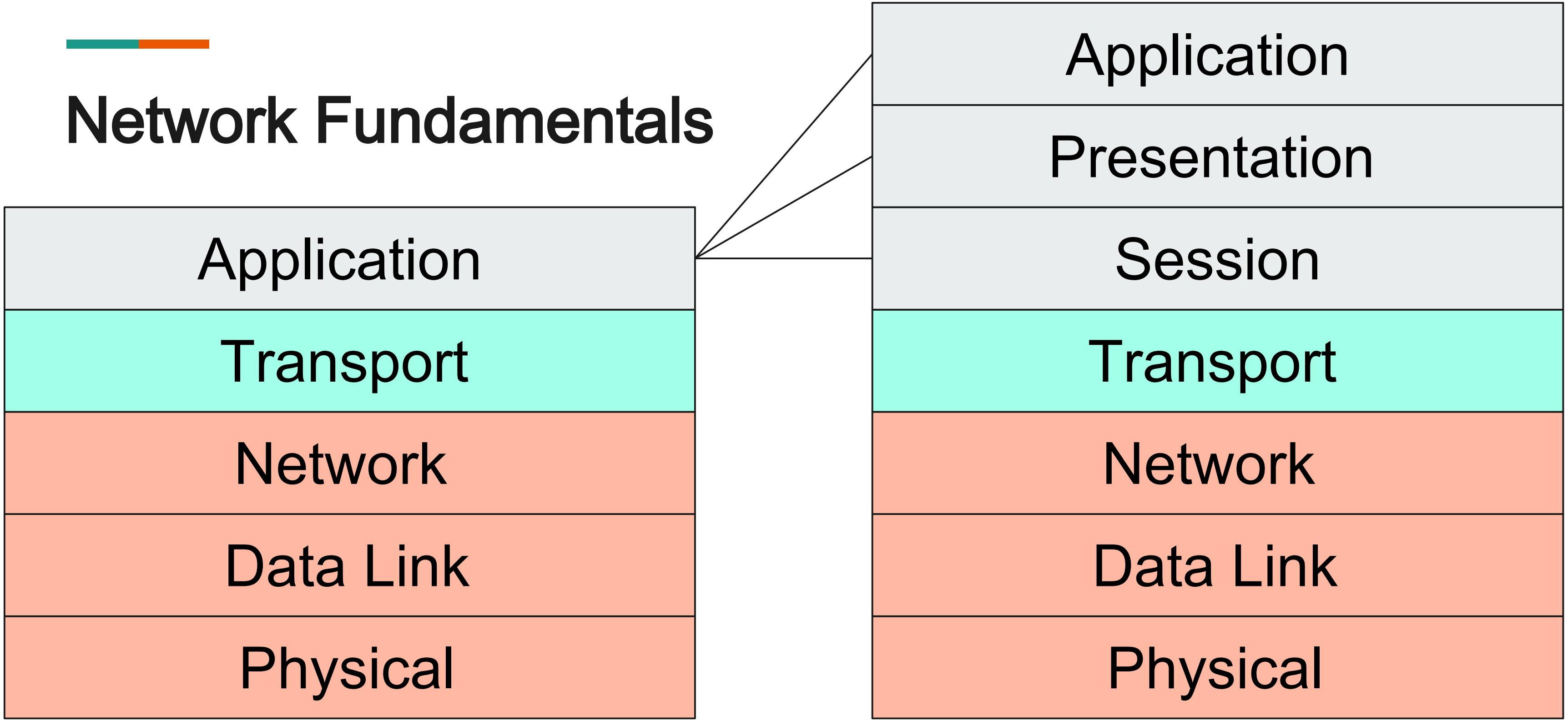
Network

Data Link

Physical

OSI Model

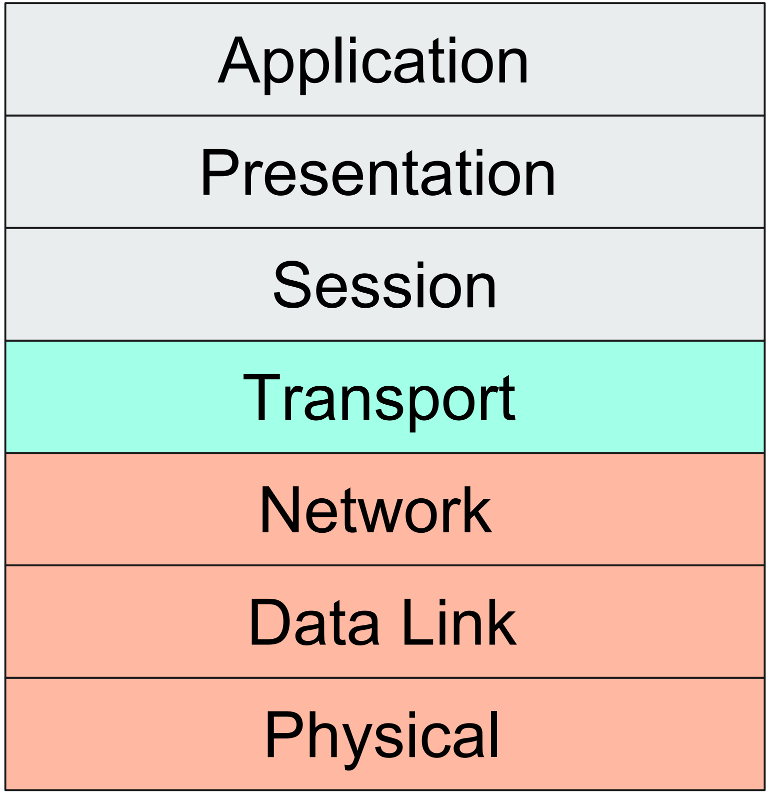
Network Fundamentals



5 Layer

OSI Model

Network Fundamentals



Application

Presentation

Session

Transport

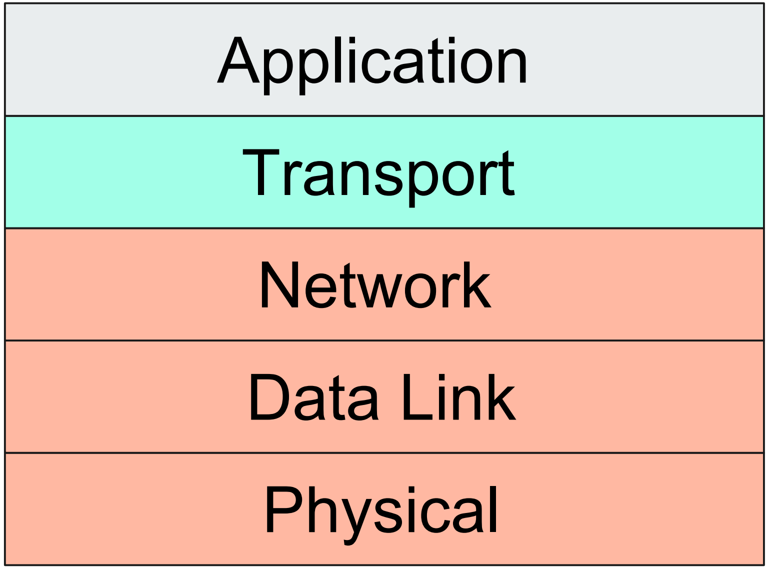
Network

Data Link

Physical

OSI Model

Network Fundamentals



Application

Transport

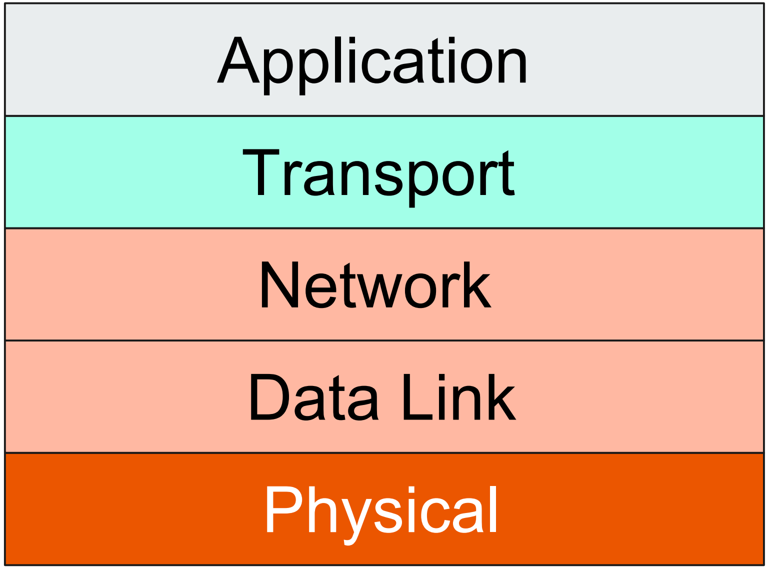
Network

Data Link

Physical

5 Layer

Physical



Application

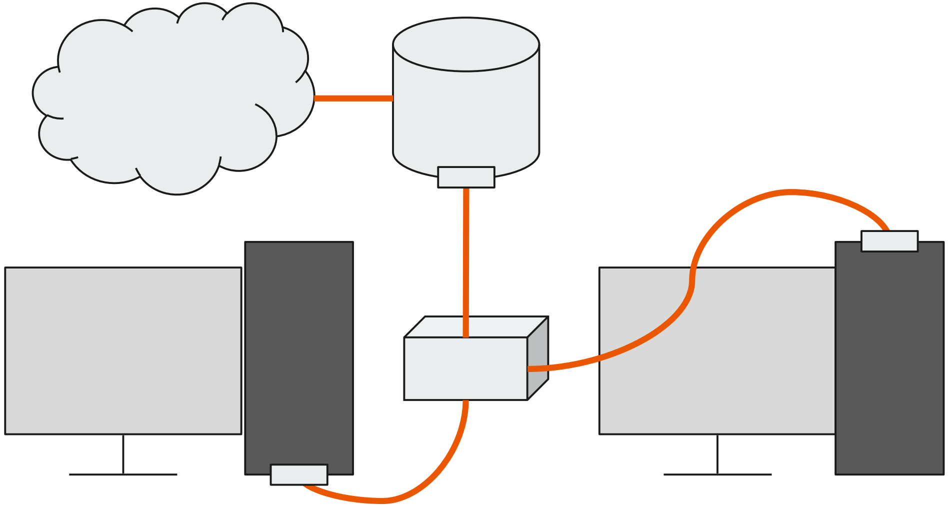
Transport

Network

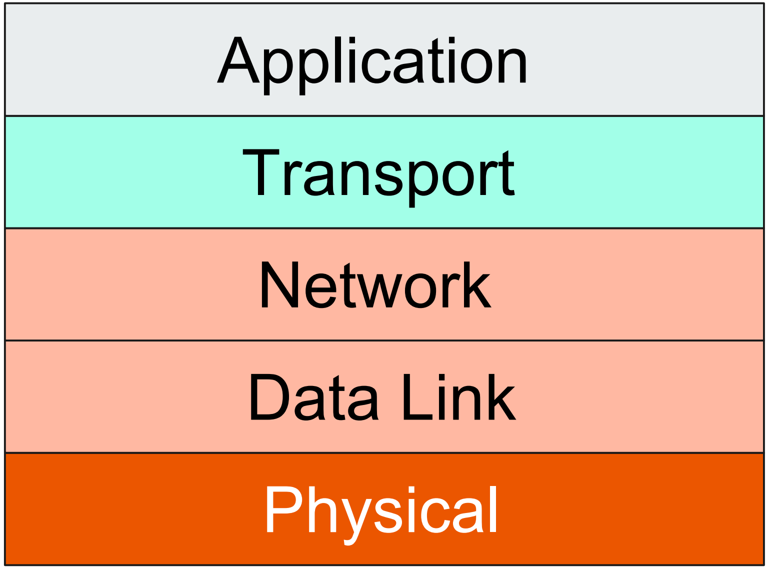
Data Link

Physical

- The hard link between machines.



Physical



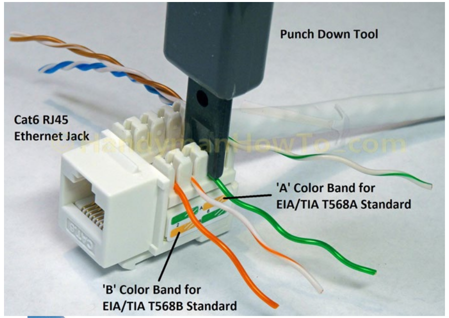
Application

Transport

Network

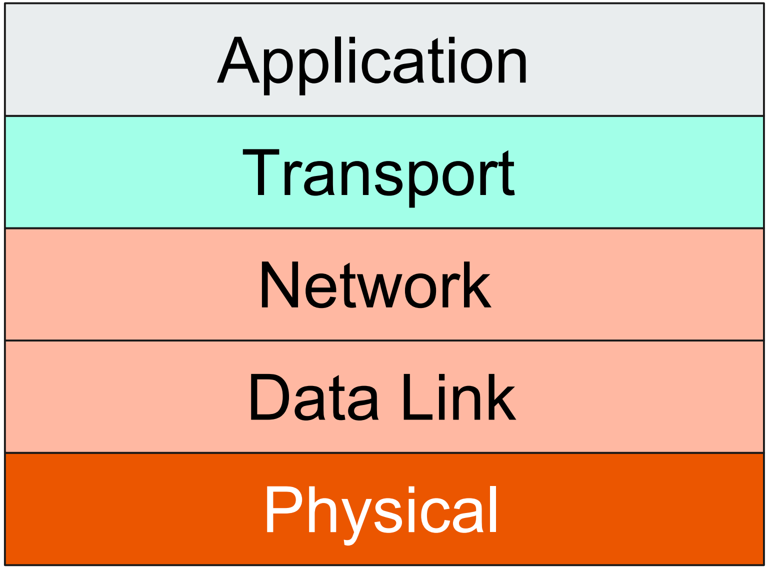
Data Link

Physical


Punch Down Tool
Cat6 RJ45 Ethernet Jack
'A' Color Band for EIA/TIA T568A Standard
'B' Color Band for EIA/TIA T568B Standard

https://www.goodfreephotos.com/albums/vector-images/wifi-connection-symbol-vector-file.png
https://www.handymanhowto.com/wp-content/uploads/2016/12/Cat6-Ethernet-Jack-Punchdown-Wiring.jpg
https://www.parts-express.com/Data/Default/Images/Catalog/Original/150-714_HR_0.jpg

Physical



Application

Transport

Network

Data Link

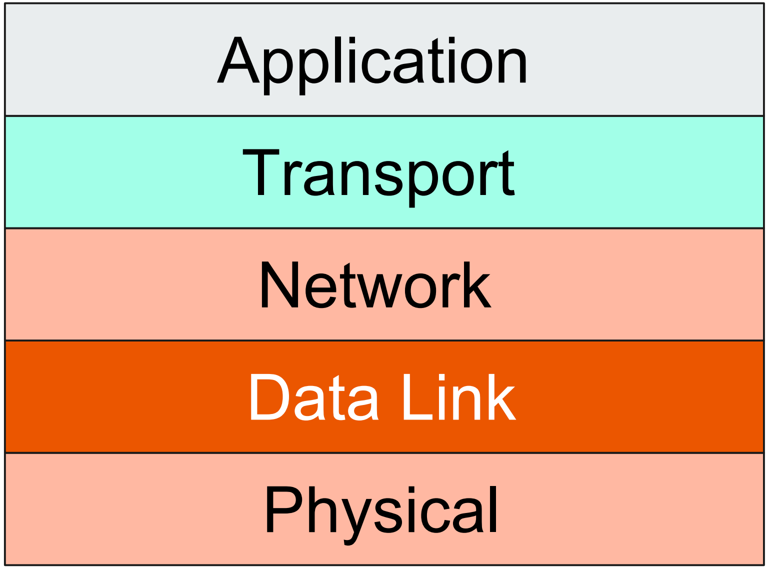
Physical

How do we secure this?

- Wired
  - Disconnect it.
  - Fiber instead of ethernet.
- Wireless
  - WPA3 (WPA2 KRACK)
  - Appropriate zoning

Other ideas?

Data Link



Application

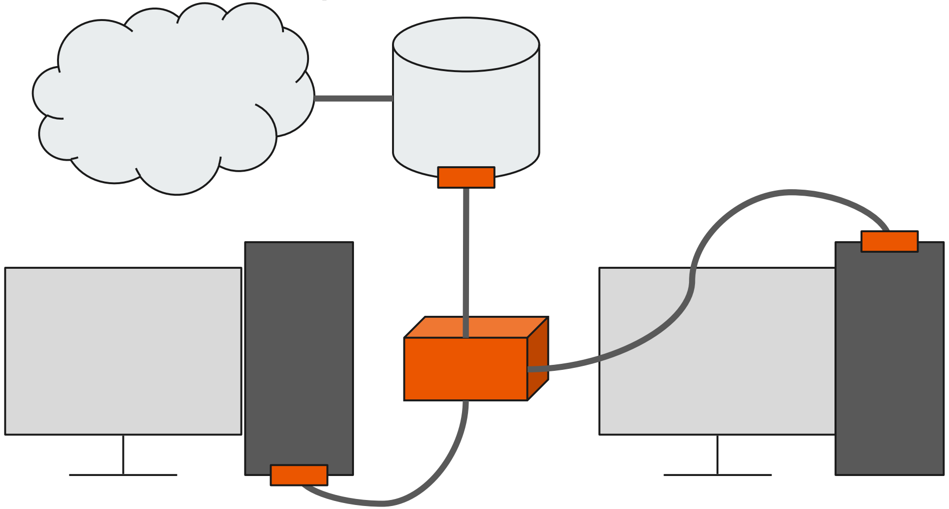
Transport

Network

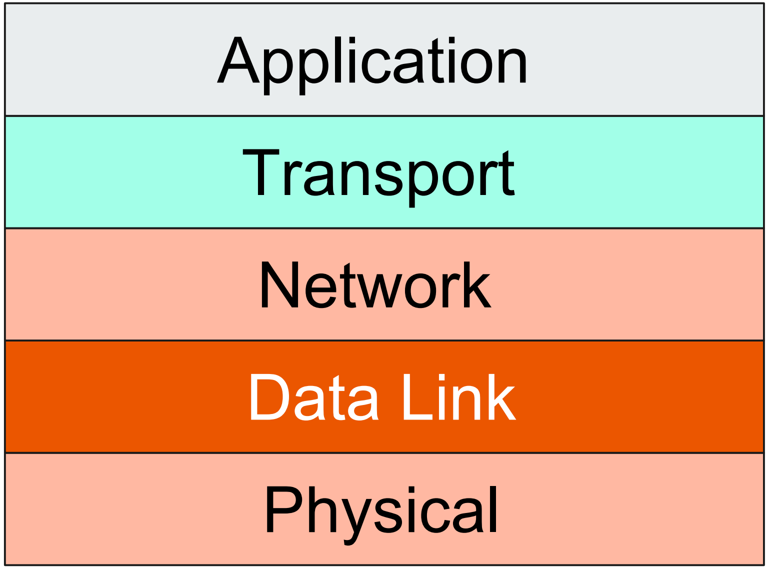
Data Link

Physical

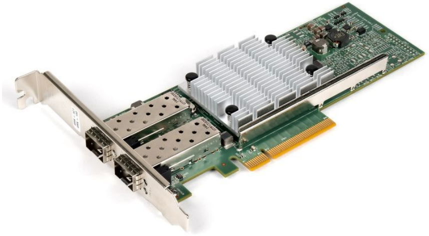
- The physical identity of devices.
- Example: 01:34:67:9A:CD:F0

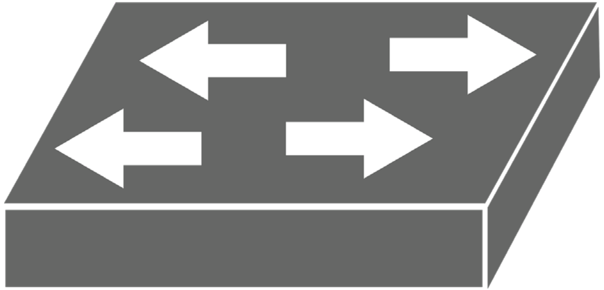


Data Link



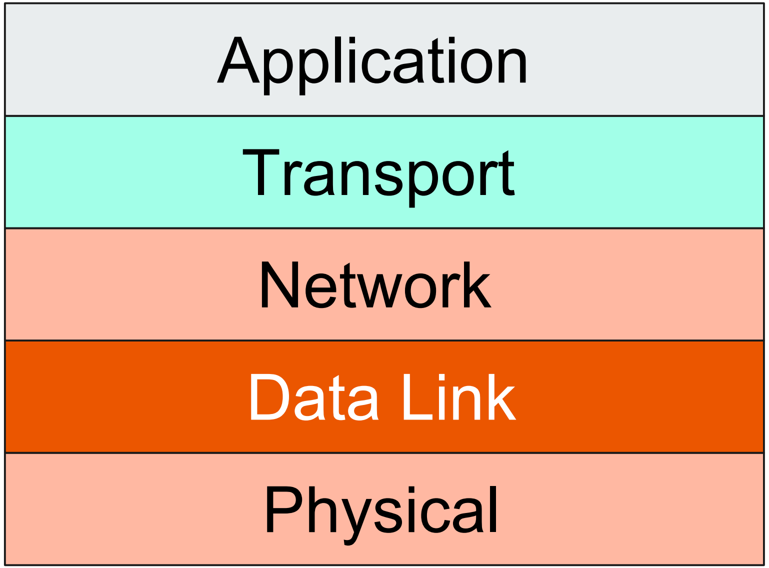
00:82:05:9A:D3:BD





https://icon-library.net/images/switch-icon-png/switch-icon-png-25.jpg
https://www.lifewire.com/thmb/wSluszBhz3JJi_9DRVhXAP1PJ58=/768x0/filters:no_upscale():max_bytes(150000):strip_icc()/Qle3442-cu_10gbe_nic-5aee673cff1b780036491a47.jpg
https://www.bluetooth.com/wp-content/uploads/2019/04/Bluetooth_FM_Color.png

Data Link



Application

Transport

Network

Data Link

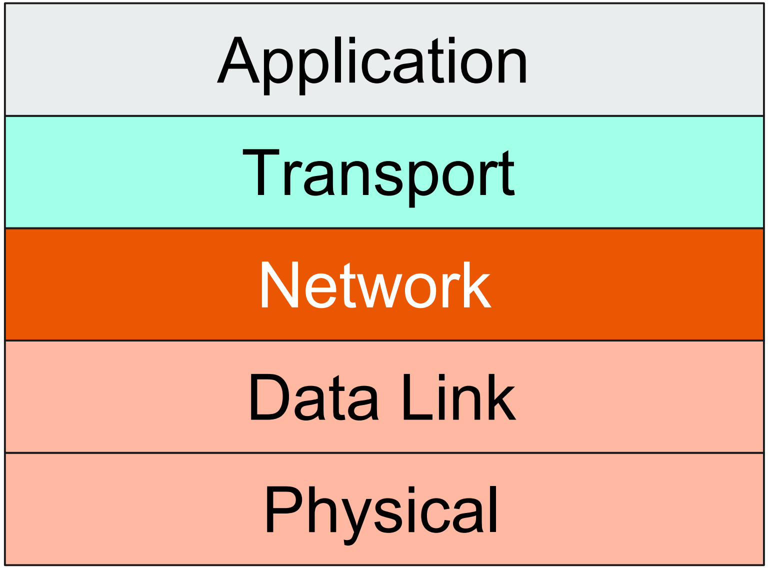
Physical

How do we secure this?

- What can be done:
  - Encryption (VLANs)
  - Flood prevention
- What cannot be solved:
  - Spoofing can be detected but not resolved.

    Others ideas?

Network



Application

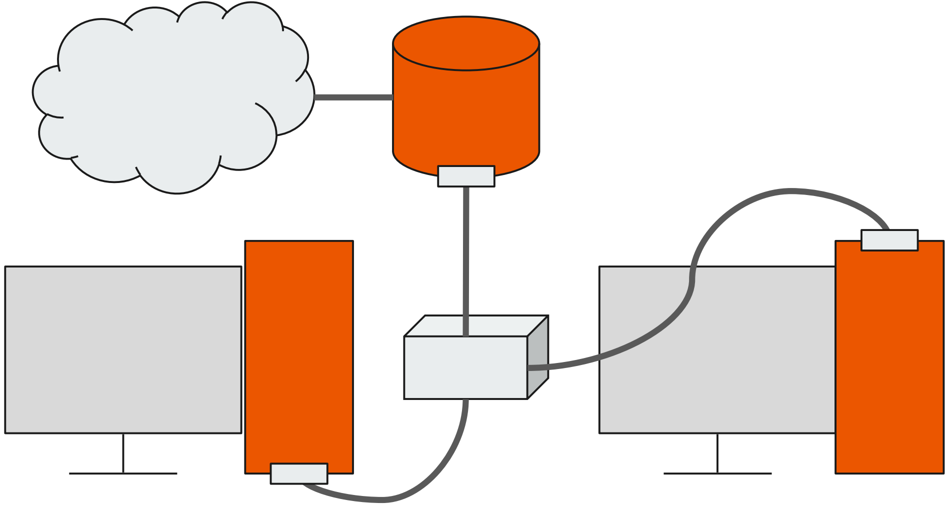
Transport

Network

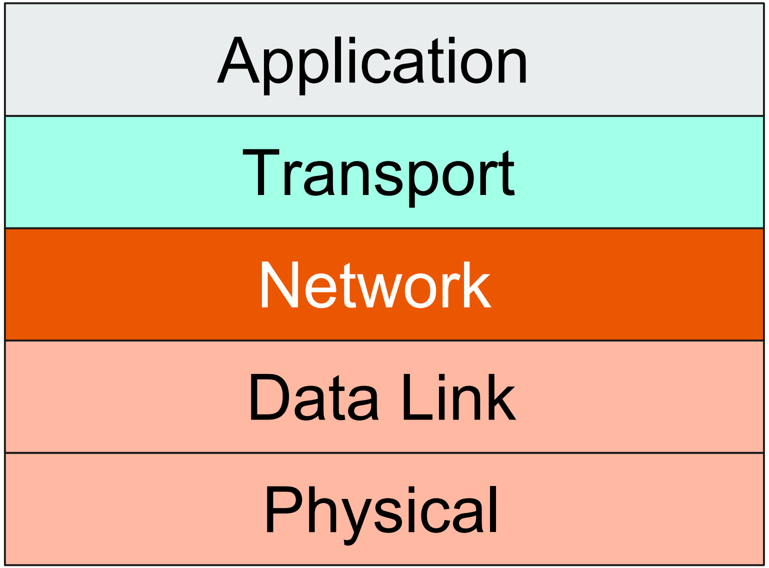
Data Link

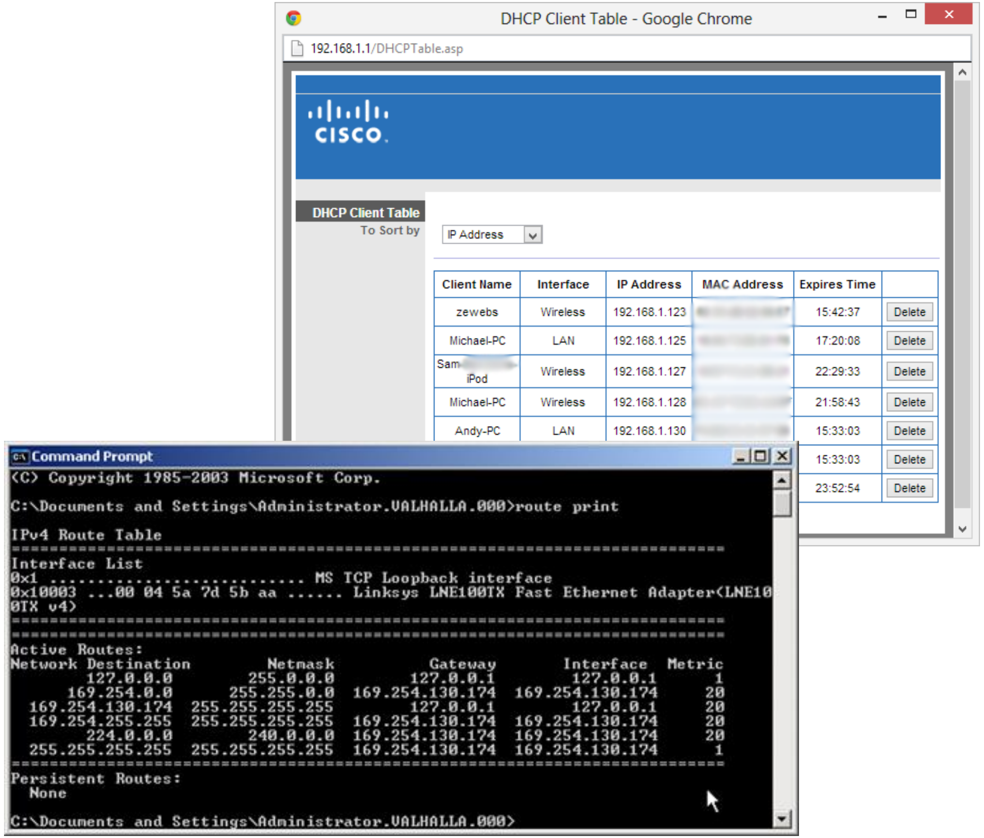
Physical

- The identity within a network
- The identity between networks



Network





192.168.1.1/DHCPTable.asp

DHCP Client Table

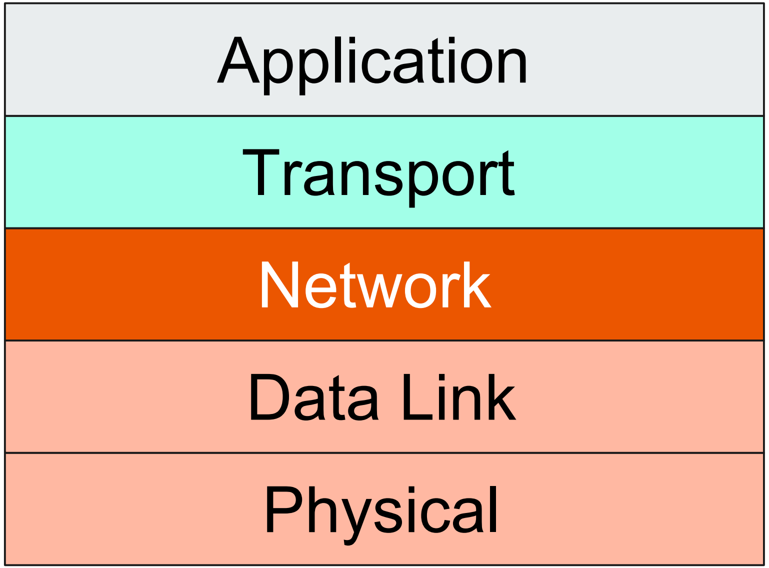
To Sort by: IP Address

Client Name	Interface	IP Address	MAC Address	Expires Time	
zewebs	Wireless	192.168.1.123	[redacted]	15:42:37	Delete
Michael-PC	LAN	192.168.1.125	[redacted]	17:20:08	Delete
Sam[redacted] iPod	Wireless	192.168.1.127	[redacted]	22:29:33	Delete
Michael-PC	Wireless	192.168.1.128	[redacted]	21:58:43	Delete
Andy-PC	LAN	192.168.1.130	[redacted]	15:33:03	Delete
				15:33:03	Delete
				23:52:54	Delete

```
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator.VALHALLA.000>route print

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 04 5a 7d 5b aa ...... Linksys LNE100TX Fast Ethernet Adapter(LNE10
0TX v4)
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      169.254.0.0      255.255.0.0  169.254.130.174 169.254.130.174      20
  169.254.130.174  255.255.255.255        127.0.0.1       127.0.0.1      20
  169.254.255.255  255.255.255.255  169.254.130.174 169.254.130.174      20
        224.0.0.0        240.0.0.0  169.254.130.174 169.254.130.174      20
  255.255.255.255  255.255.255.255  169.254.130.174 169.254.130.174       1
===========================================================================
Persistent Routes:
  None

C:\Documents and Settings\Administrator.VALHALLA.000>
```

https://i.stack.imgur.com/mjLjP.png
https://www.sqa.org.uk/e-learning/NetInf104CD/images/pic004.jpg

Network



Application

Transport

Network

Data Link

Physical

How do we secure this?

- Firewalls!
  - Filtering
  - Zoning
- Routers
  - Proper configuration
  - Private vs. public IPs

Other ideas?

Transport

Application

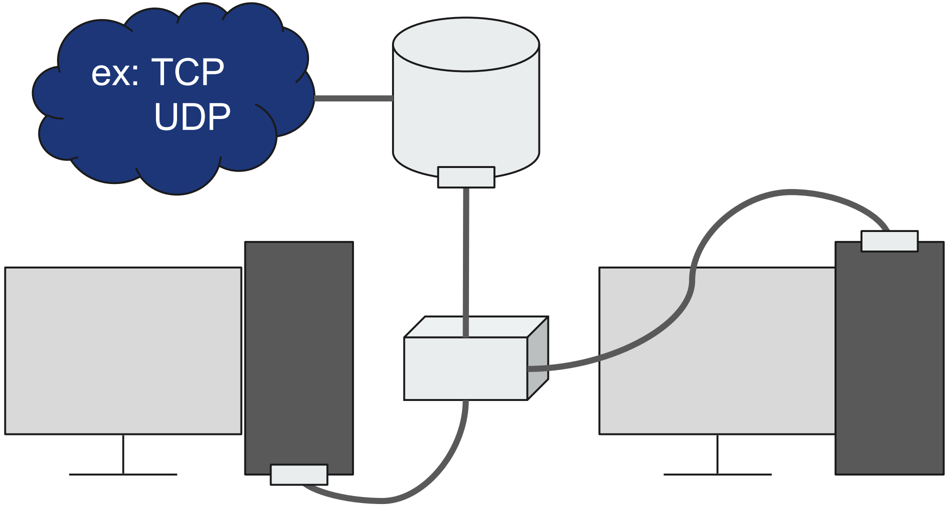
Transport

Network

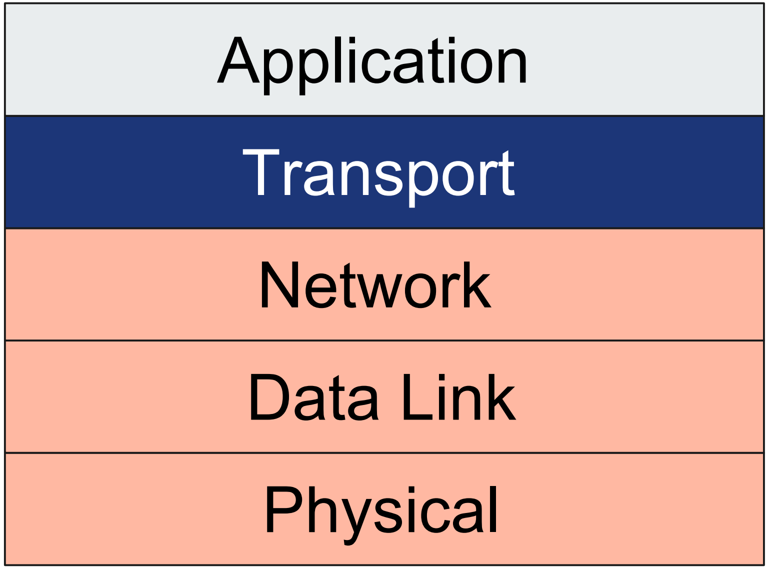
Data Link

Physical

- The protocols to communicate



Transport



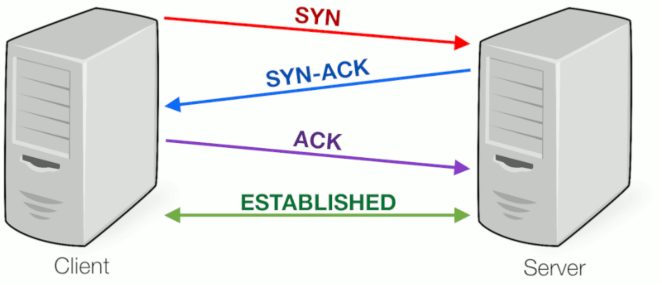
Application

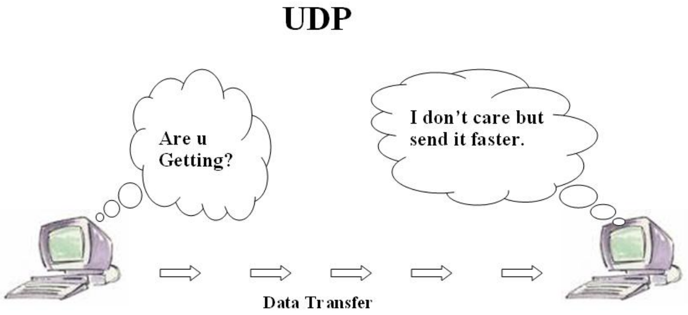
Transport

Network

Data Link

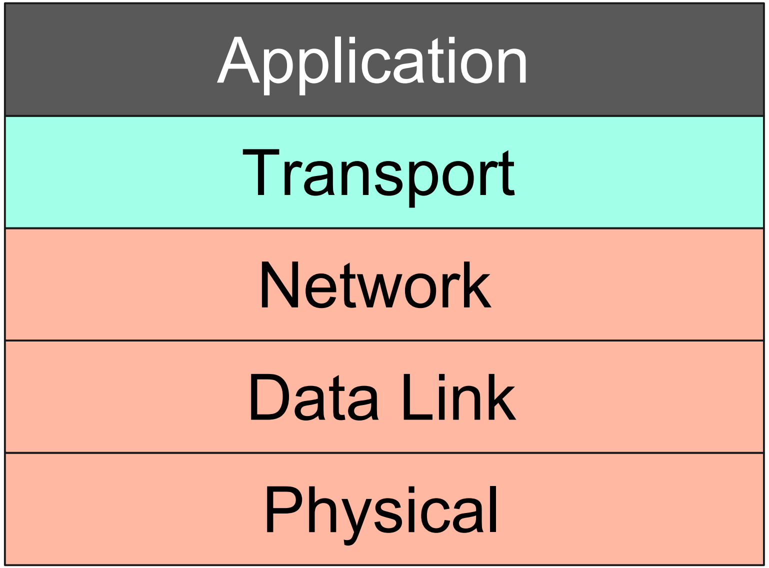
Physical





https://www.coengoedegebure.com/content/images/2018/09/handshake.png
https://upload.wikimedia.org/wikipedia/commons/0/0f/Fig2_UDPwork.jpg

Application and Everything Else



Application

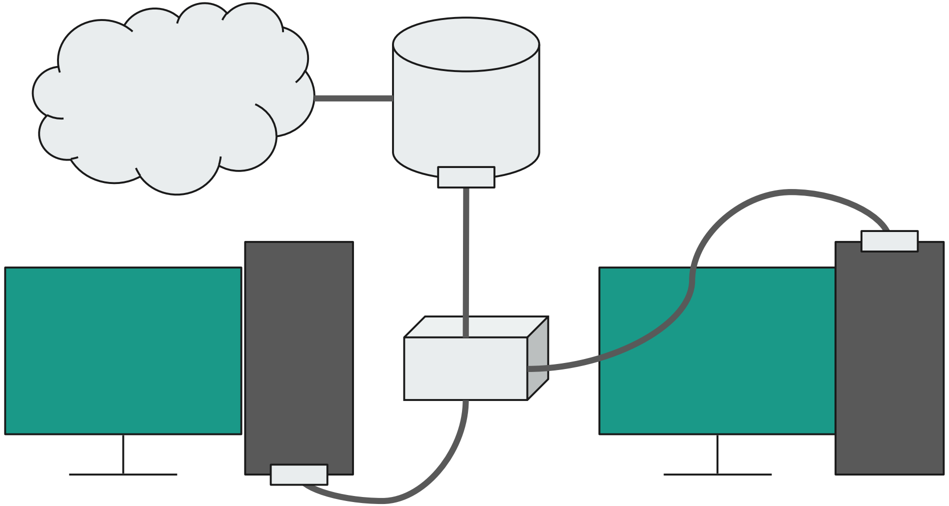
Transport

Network

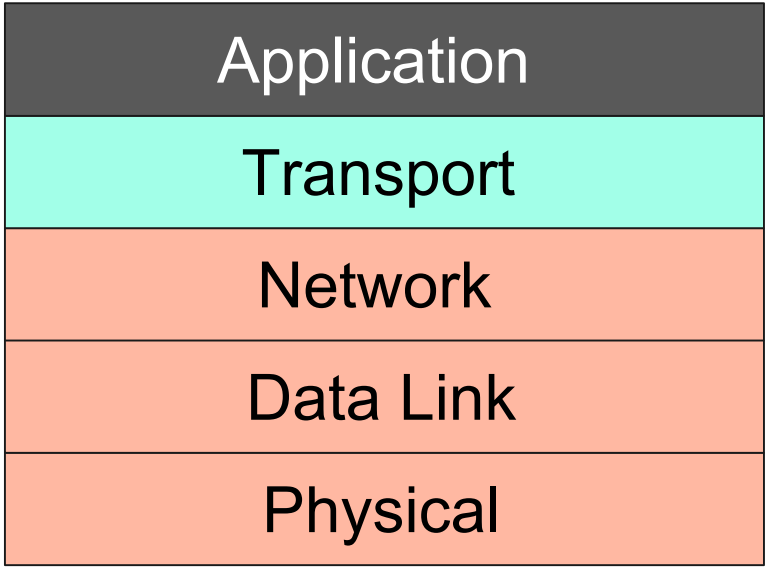
Data Link

Physical

- Programs using networks



Application and Everything Else



Application

Transport

Network

Data Link

Physical

https://cdn.vox-cdn.com/thumbor/AyclQrzQvrHuoZLJNa6LVYZ1zMA=/0x0:1280x720/1200x800/filters:focal(538x258:742x462)/cdn.vox-cdn.com/uploads/chorus_image/image/65311063/origin.0.jpg
https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/IMessage_logo.svg/1024px-IMessage_logo.svg.png
https://regmedia.co.uk/2017/07/28/shutterstock_facebook3.jpg?x=442&y=293&crop=1

Tools

Some useful tools for analyzing network traffic.

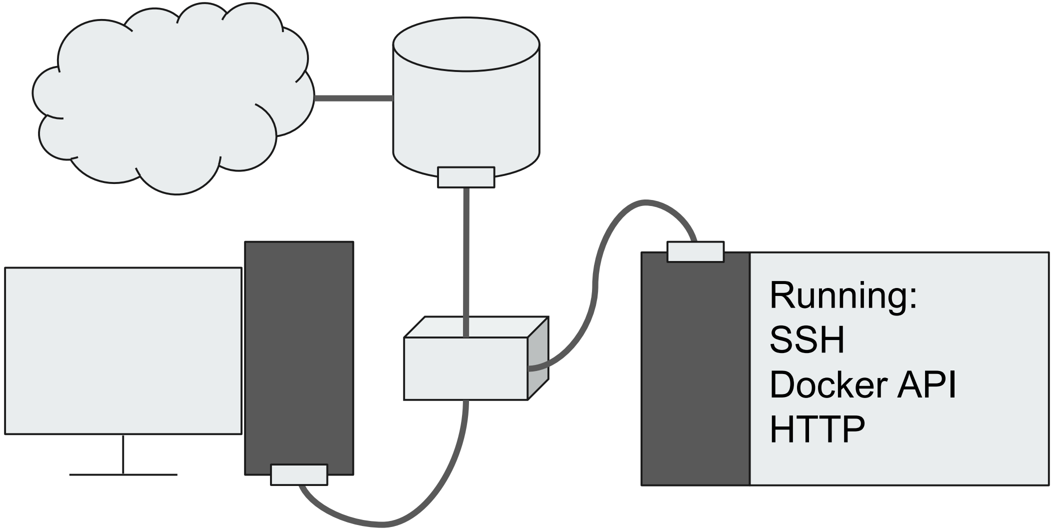
- ping - Sends ICMP Echo Request packets
- netcat (nc) - Lets you send arbitrary data over TCP or UDP
- tcpdump - captures and dumps traffic on a network interface
- tshark - more featureful tcpdump
- Wireshark - GUI tool to create and analyze packet captures
- curl/wget/httpie - let you make lots of HTTP requests
- nmap - network mapper (more on this later)
- scapy - Python library to do all kinds of things with packets

Network Security

Least Privilege

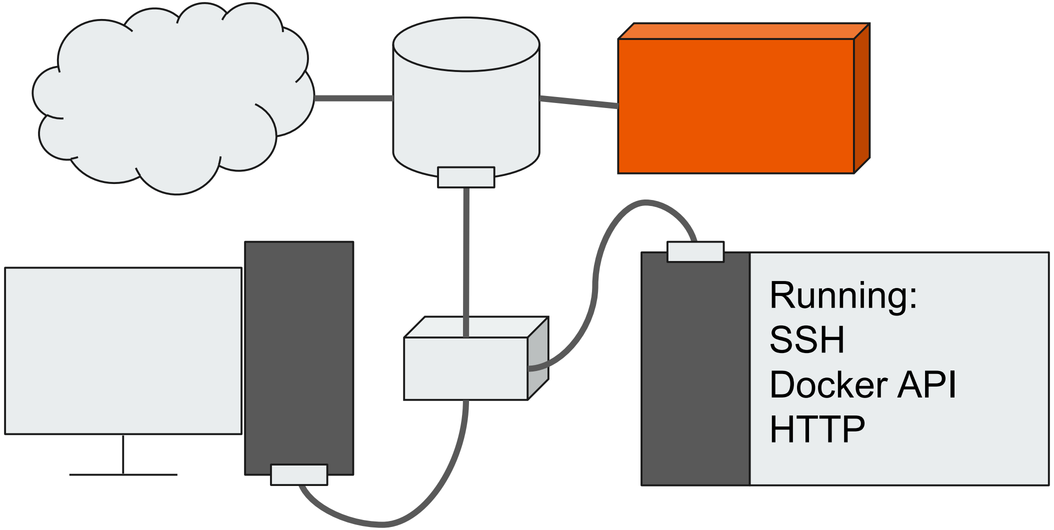
- Maintain availability while being as close to disconnected as possible.
- Minimums required for operation:
  - Minimum permissions
  - Minimum services
  - Minimum access

Least Privilege Example



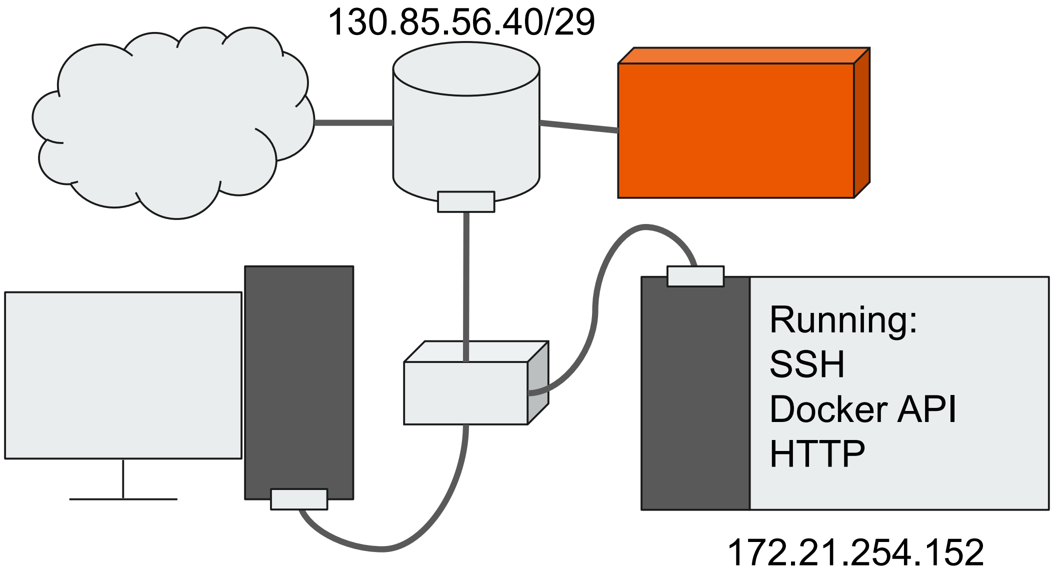
Running:
SSH
Docker API
HTTP

Least Privilege Example

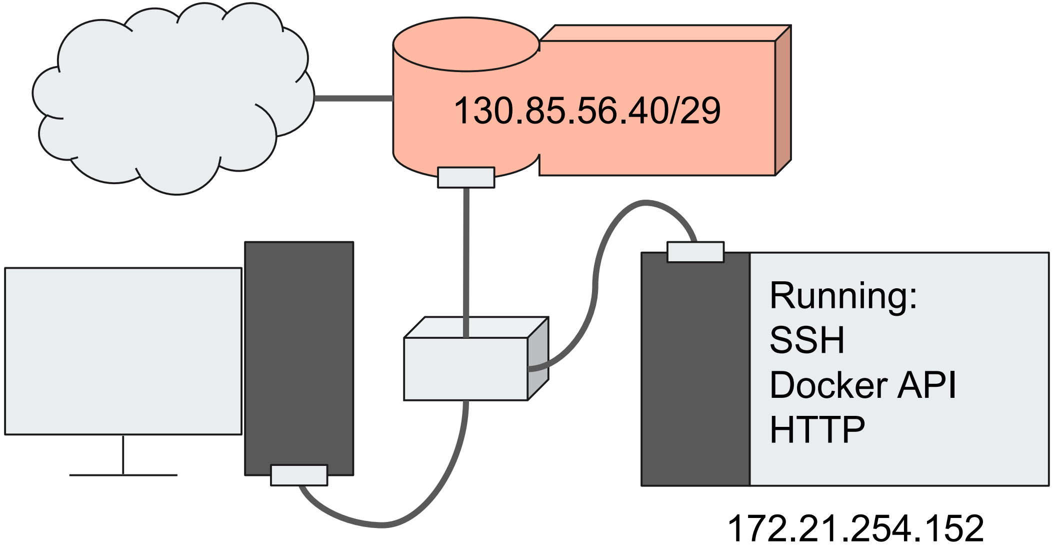


Running:
SSH
Docker API
HTTP

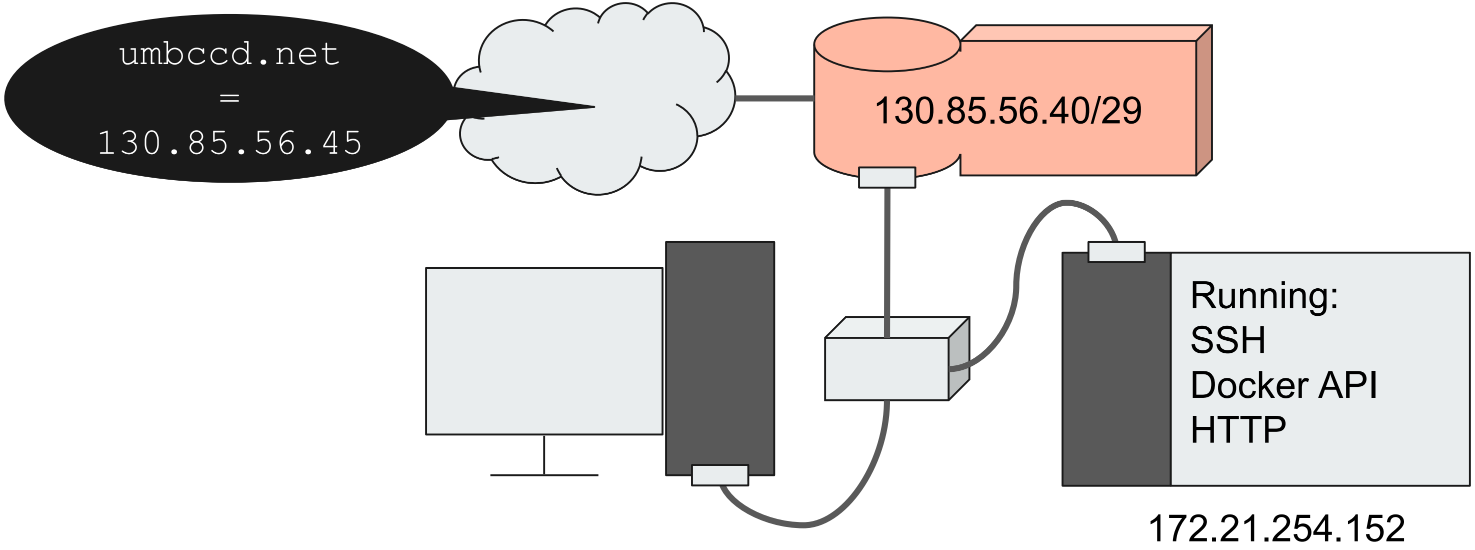
Least Privilege Example



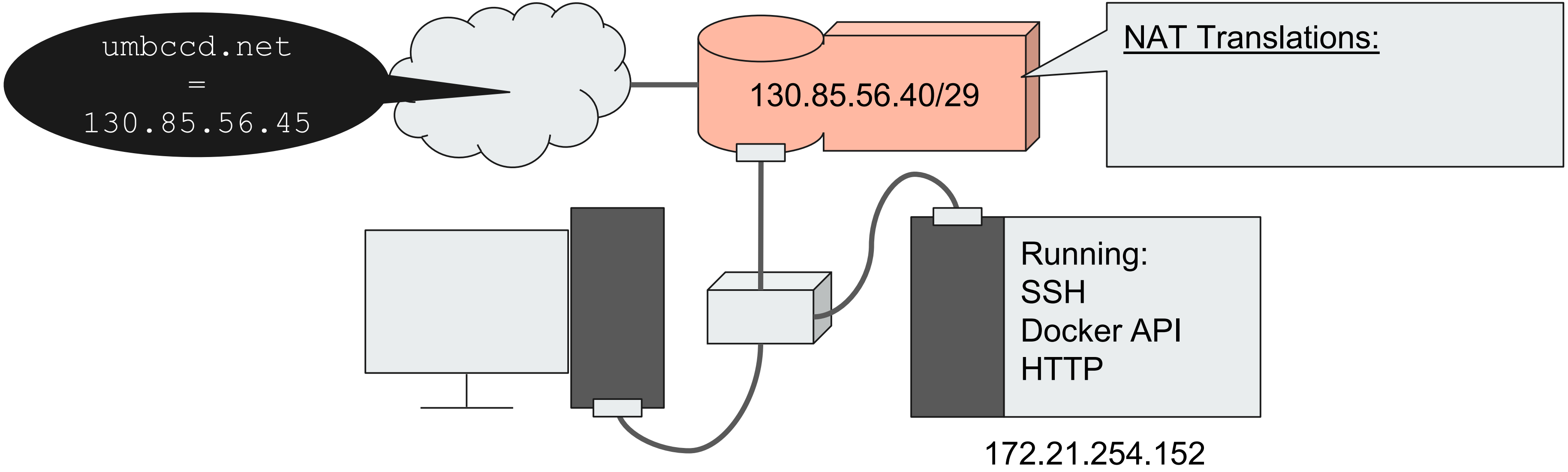
Least Privilege Example



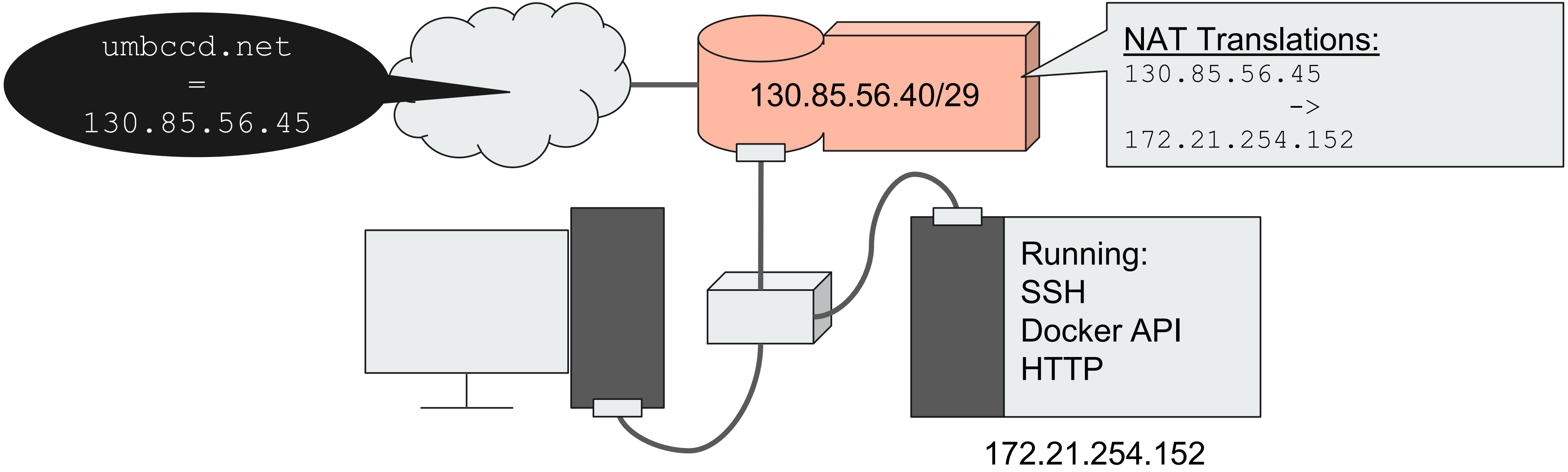
Least Privilege Example



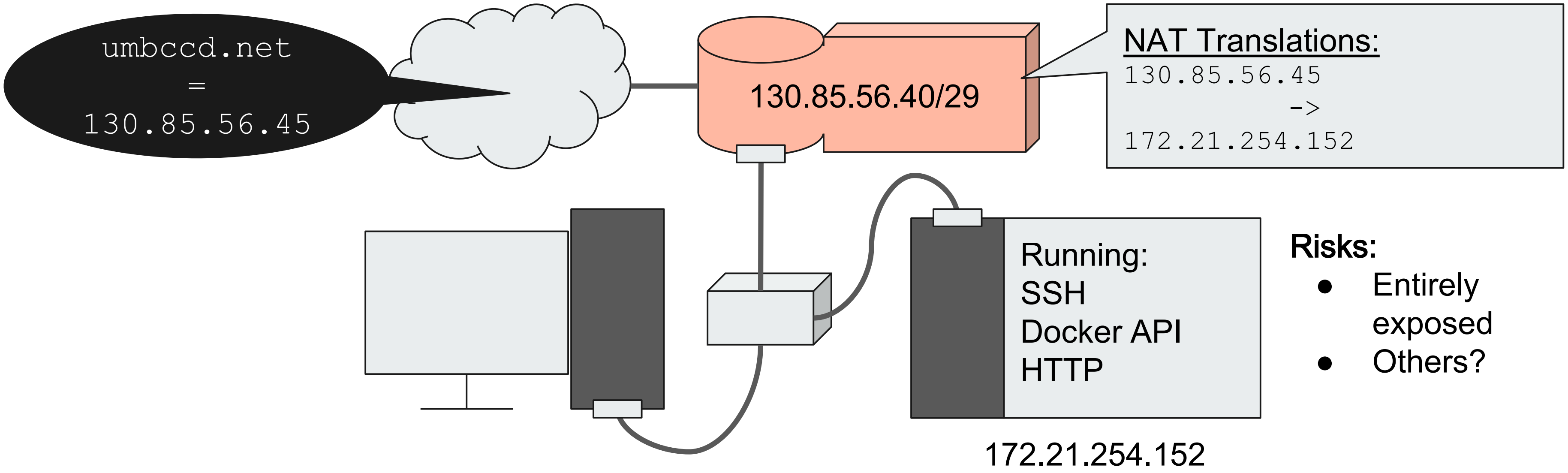
Least Privilege Example



Least Privilege Example



Least Privilege Example



umbccd.net
=
130.85.56.45

130.85.56.40/29

NAT Translations:
130.85.56.45
->
172.21.254.152

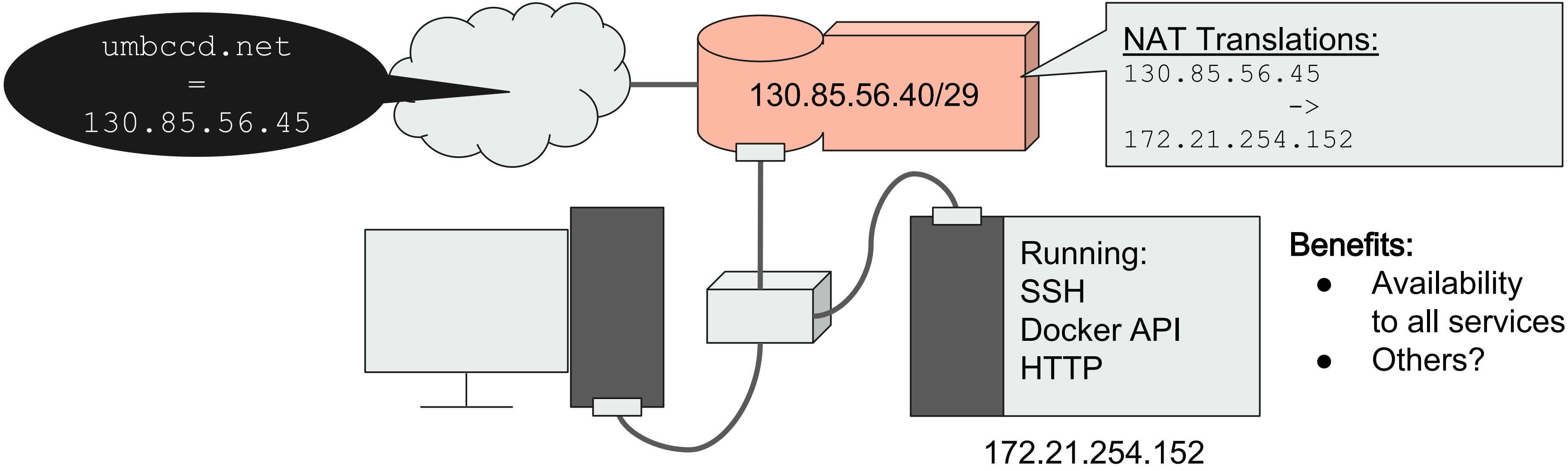
Running:
SSH
Docker API
HTTP

172.21.254.152

Risks:

- Entirely exposed
- Others?

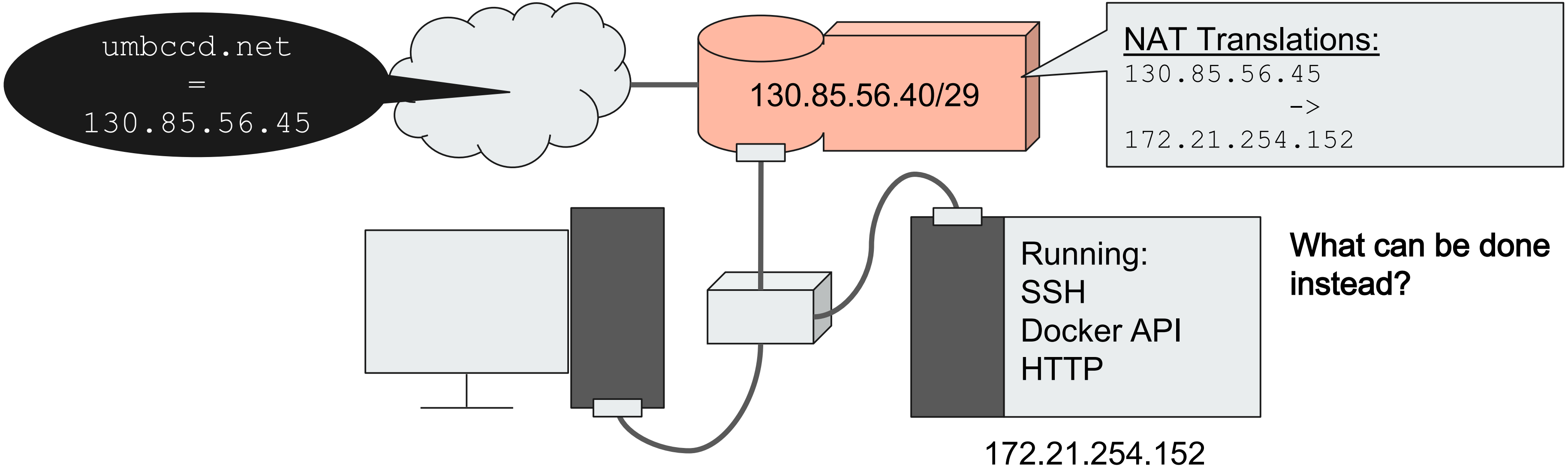
Least Privilege Example



Benefits:

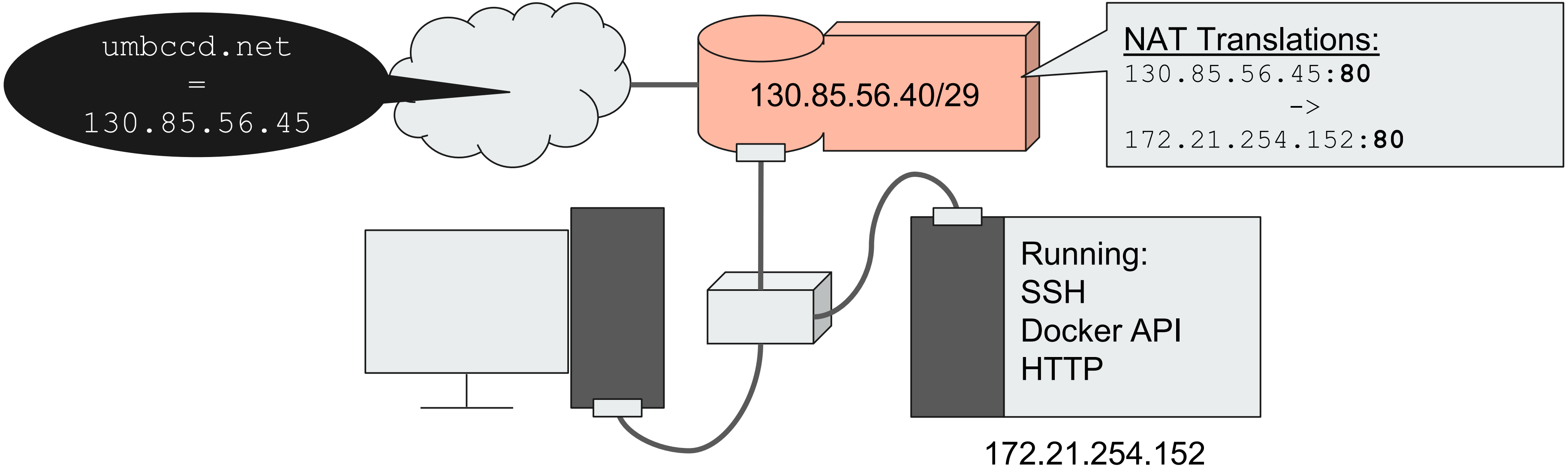
- Availability to all services
- Others?

Least Privilege Example

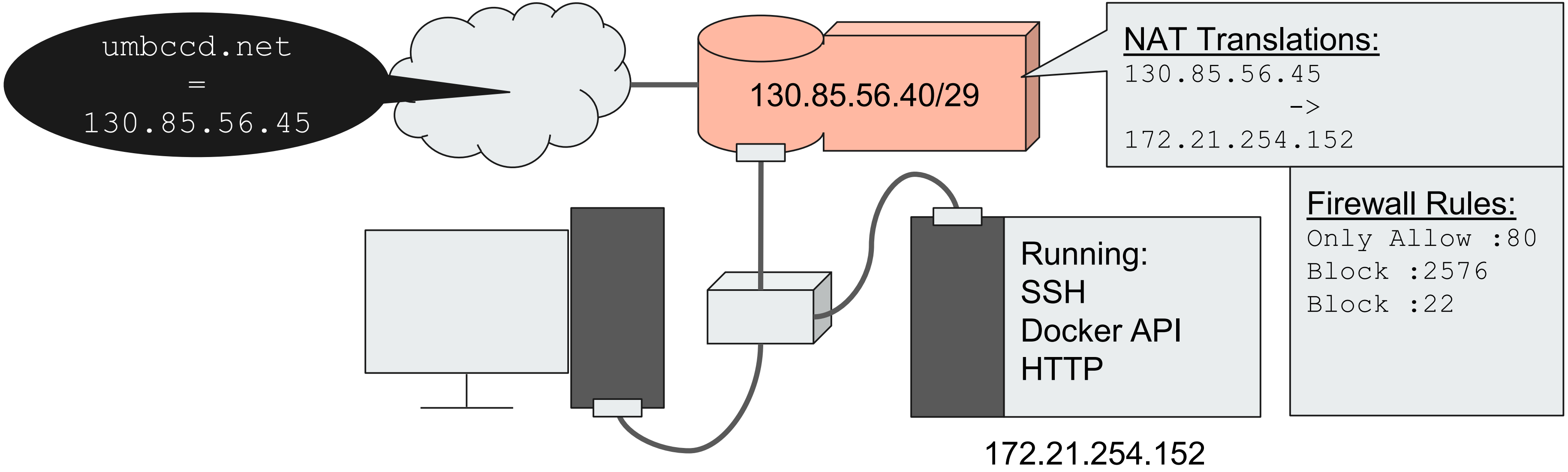


What can be done instead?

Least Privilege Solution 1



Least Privilege Solution 2



NAT Translations:
```
130.85.56.45
        ->
172.21.254.152
```

Running:
SSH
Docker API
HTTP

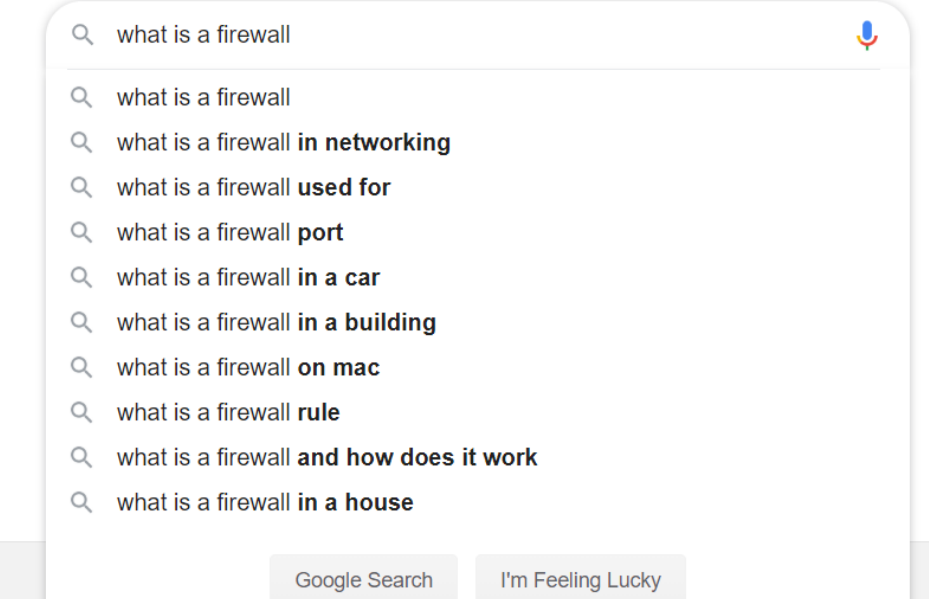
Firewall Rules:
```
Only Allow :80
Block :2576
Block :22
```

Firewalls

Firewall Firm
MANAGED FIREWALL SOLUTION PROVIDER
FORTINET
JUNIPer
NETWORKS
FORCEPOINT
POWERED BY Raytheon
Check Point
SOFTWARE TECHNOLOGIES LTD.
CISCO
HUAWEI
paloalto
NETWORKS
SONICWALL
WatchGuard
Barracuda
Reclaim your network.
SOPHOS
Security made simple.
Hillstone
NETWORKS
H3C
The Leader in Digital Solutions
SANGFOR
AhnLab

https://cdn.shortpixel.ai/client/q_lossy,ret_img/https://firewall.firm.in/wp-content/uploads/2018/09/Firewall_Banner.jpg

What is a firewall?



what is a firewall

what is a firewall

what is a firewall **in networking**

what is a firewall **used for**

what is a firewall **port**

what is a firewall **in a car**

what is a firewall **in a building**

what is a firewall **on mac**

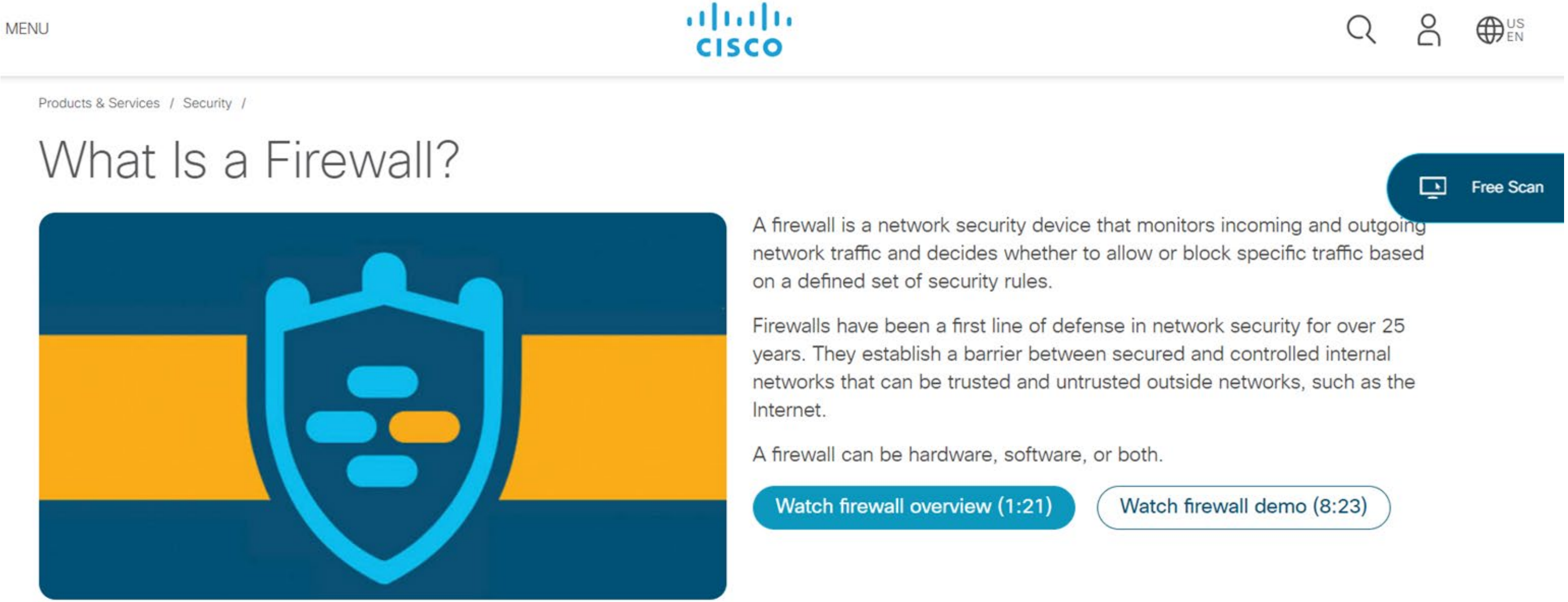
what is a firewall **rule**

what is a firewall **and how does it work**

what is a firewall **in a house**

google.com

What is a firewall?


MENU
cisco
US
EN
Products & Services / Security /
Free Scan
Watch firewall overview (1:21)
Watch firewall demo (8:23)

What Is a Firewall?

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

What is a firewall?

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Examples on Servers: iptables, ipfw, pf (packet filter), Windows Firewall.
- Capabilities:
  - Blacklist: explicitly block some content (illegal to block by IP in competitions)
  - Whitelist: explicitly allow some content
  - Filter by protocol (transport layer)
  - Conduct packet inspection (application layer)
- Can perform some capabilities of a router.

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Lab

Summary

In this lab, you will:

- be learning how to manipulate availability to improve security.
- gain experience setting up services on both Windows Server and Linux(Ubuntu)
- learn how to configure the default firewalls of both systems.

Firewalls Used in Lab

- iptables
- Windows Firewall

Linux - iptables

- Used with the **“iptables” command** .
- Primarily filters communication by **ip address** and **port** .
- Can filter by packet content.

Windows - Windows Firewall

- Used with the **Windows Firewall application** .
- Primarily manages communication of **applications** on a system.
- Can filter by ip address and port.

Linux - iptables

iptables has tables, and within each table there are chains
Default chains are INPUT, OUTPUT, and FORWARD.

Chains execute firewall filtering from top to bottom.

Sample commands:

```
          iptables -P INPUT DROP #changes the policy for the INPUT chain to DROP,
                                      which means that any rule not specify is automatically a block rule.

          iptables -A OUTPUT -i lo -j ACCEPT #allows all outbound connections to localhost.

          iptables -I INPUT -s 130.85.300.4-p tcp --dport 25 -j DROP #blocks access to SMTP from
the IP.
```

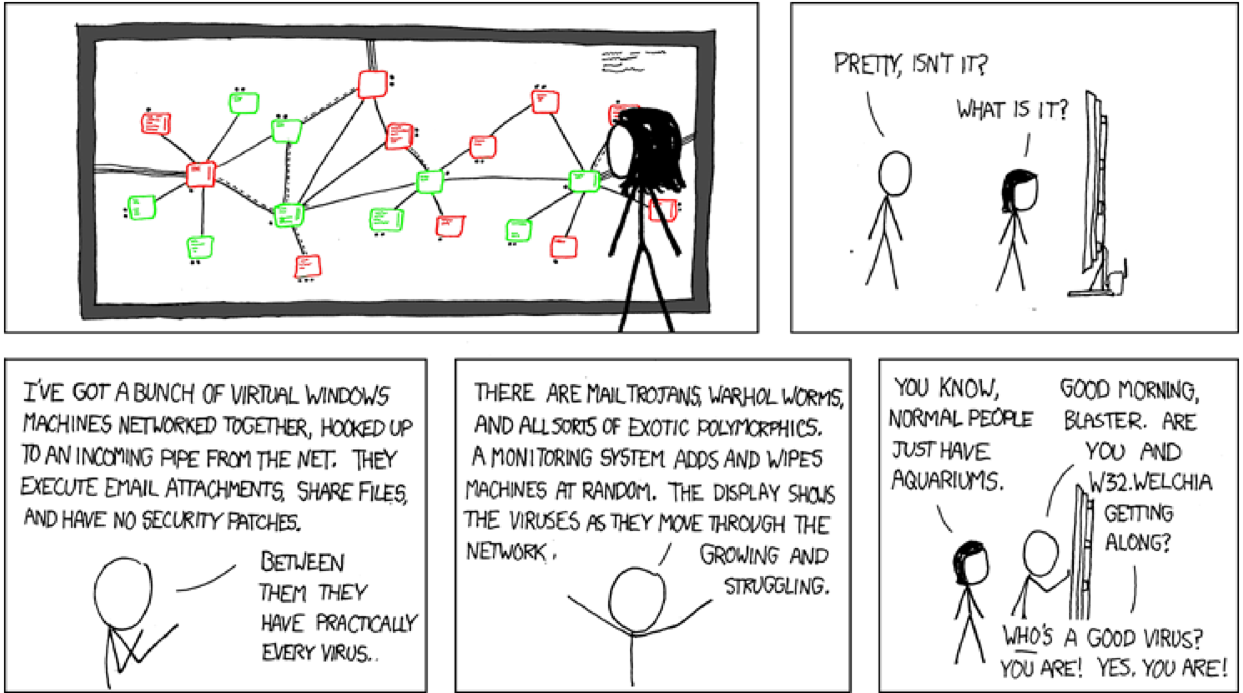
Windows - Windows Firewall

Found in Windows FIrewall, which can be searched for in the system.

Does exist.

The rules do not execute in order, simply by allow or block.

...okay, bye!


PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS..
THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK,
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!