

# Firewalls, NAT, and Intrusion Detection

---

COMPUTER SECURITY  
TARIQ ELAHI

Some slides adapted from those by Markulf Kohlweiss  
Kami Vaniea, Aggelos Kiayias, and Michael Goodrich



# Today

---

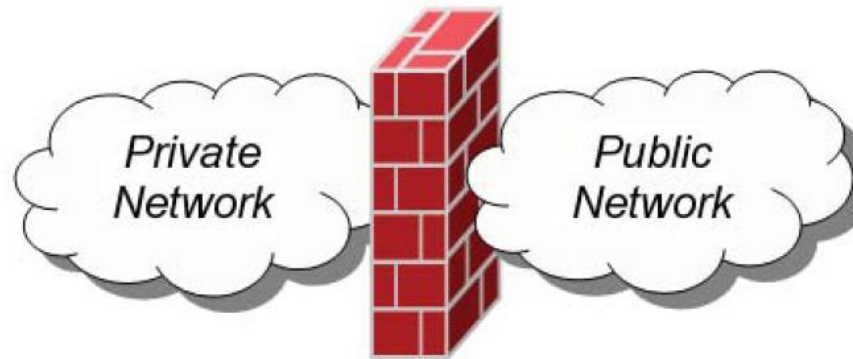
- Methods for observing, managing, and controlling network information flows
  - Firewalls
  - Network Address Translation (NAT)
  - Intrusion Detection Systems (IDS)



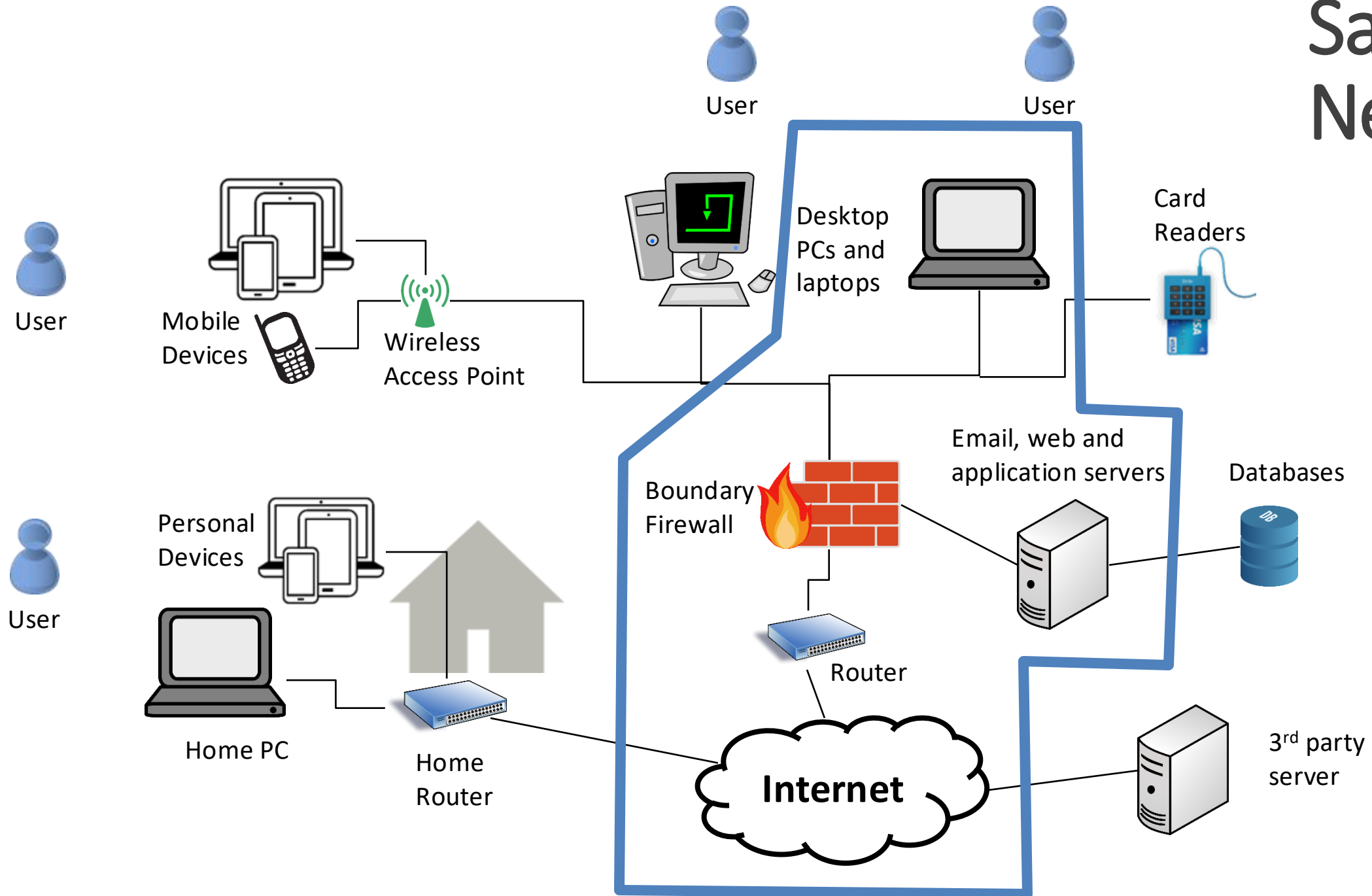
# Firewalls

---

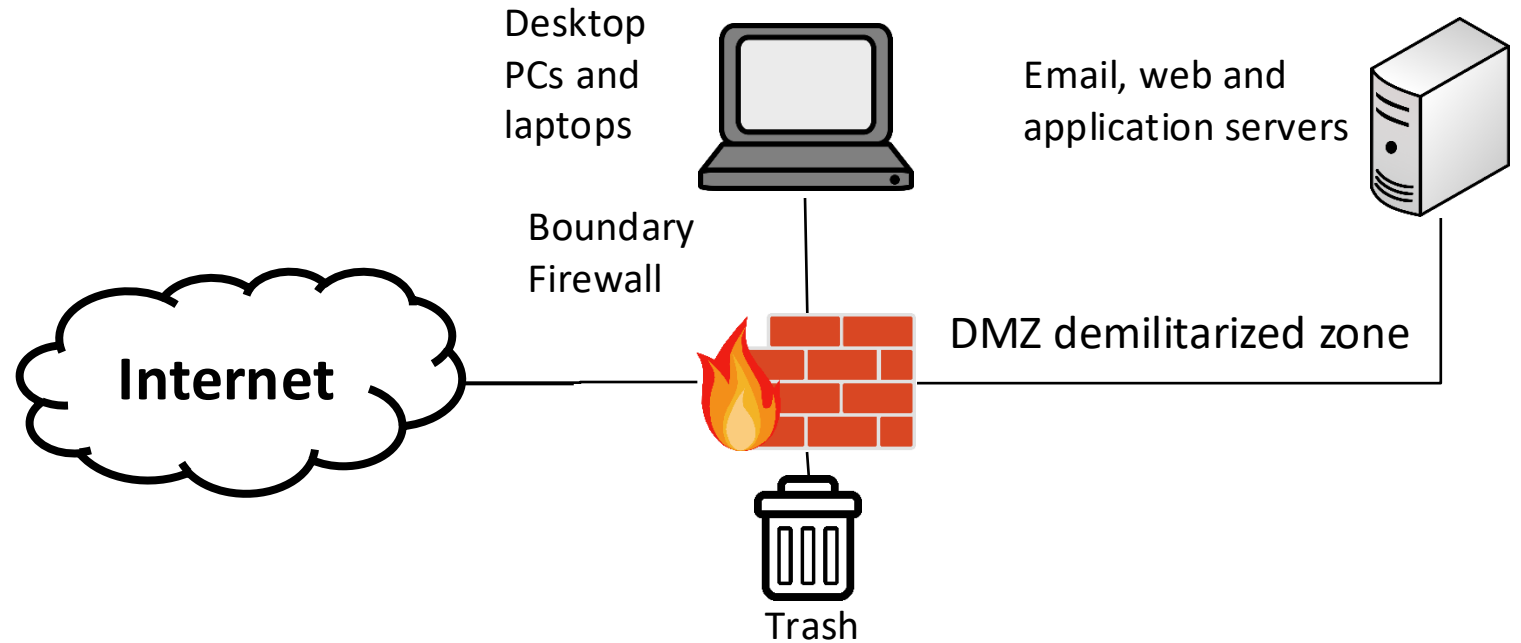
- A **firewall** is a security measure designed to prevent **unauthorized electronic access** to a networked computer system.
- Intuition: Similar to firewalls in building construction. Intent is to isolate one “network” or “compartment “ from another.



# Sample Network



- Malicious actions from the **Internet** AND **local network**
- Firewall applies a set of rules called **firewall policies**
- Based on rules, it allows or denies the traffic
- **Blocklist:**  
**Allow-by-default**
- **Allowlist:**  
**Deny-by-default**



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	22	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	UDP	*	192.168.1.*	*	Deny



# Custom Firewall ruleset from a home router

```
root@ars-router: ~  
##### Service rules  
# OpenVPN  
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT  
  
# ssh - drop any IP that tries more than 10 connections per minute  
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DE  
FAULT --mask 255.255.255.255 --rsource  
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seco  
nds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP  
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT  
  
# www - accept from LAN  
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT  
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT  
  
# DNS - accept from LAN  
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT  
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT  
  
# default drop because I'm awesome  
-A INPUT -j DROP  
  
##### forwarding ruleset
```

Image:

<http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/>  
<https://arstechnica.com/gadgets/2016/04/the-ars-guide-to-building-a-linux-router-from-scratch/>



# Firewall Types

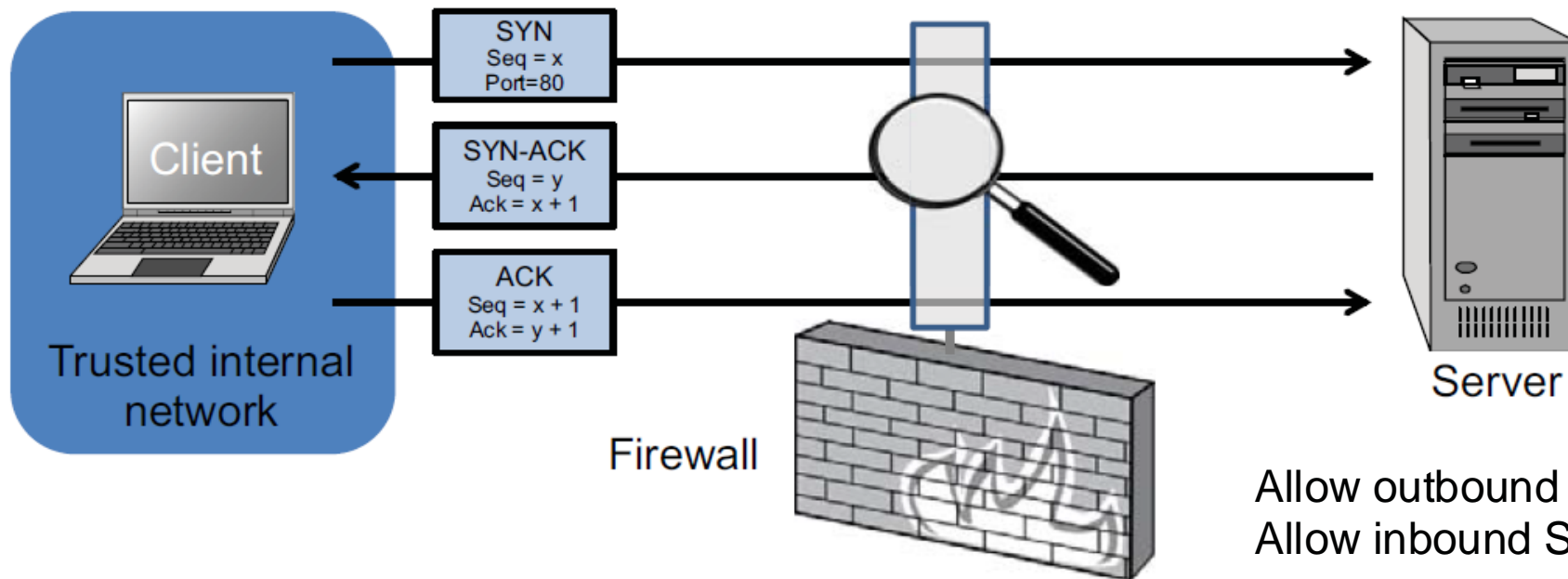
---

- **packet filters (stateless)**
  - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **stateful filters**
  - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
  - It works like a **proxy** it can “understand” certain applications and protocols.
  - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)



# Stateless Firewalls

- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



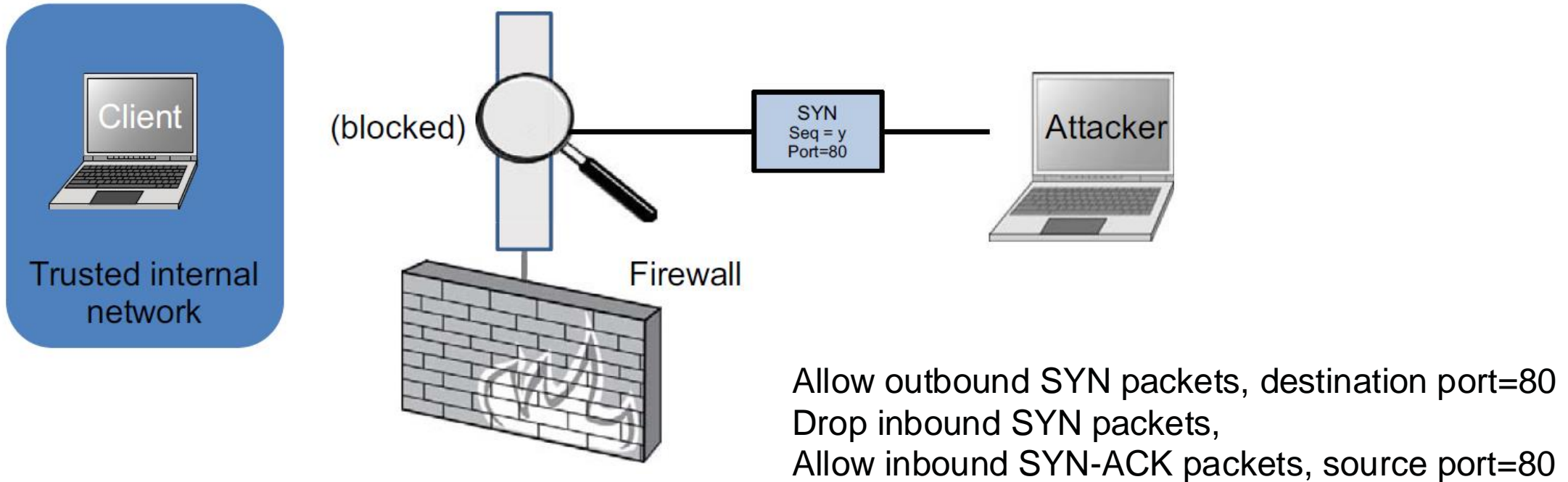
Allow outbound SYN packets, destination port=80  
Allow inbound SYN-ACK packets, source port=80





# Stateless Restrictions

- Stateless firewalls may have to be fairly restrictive in order to prevent most attacks.



# Stateful Firewalls

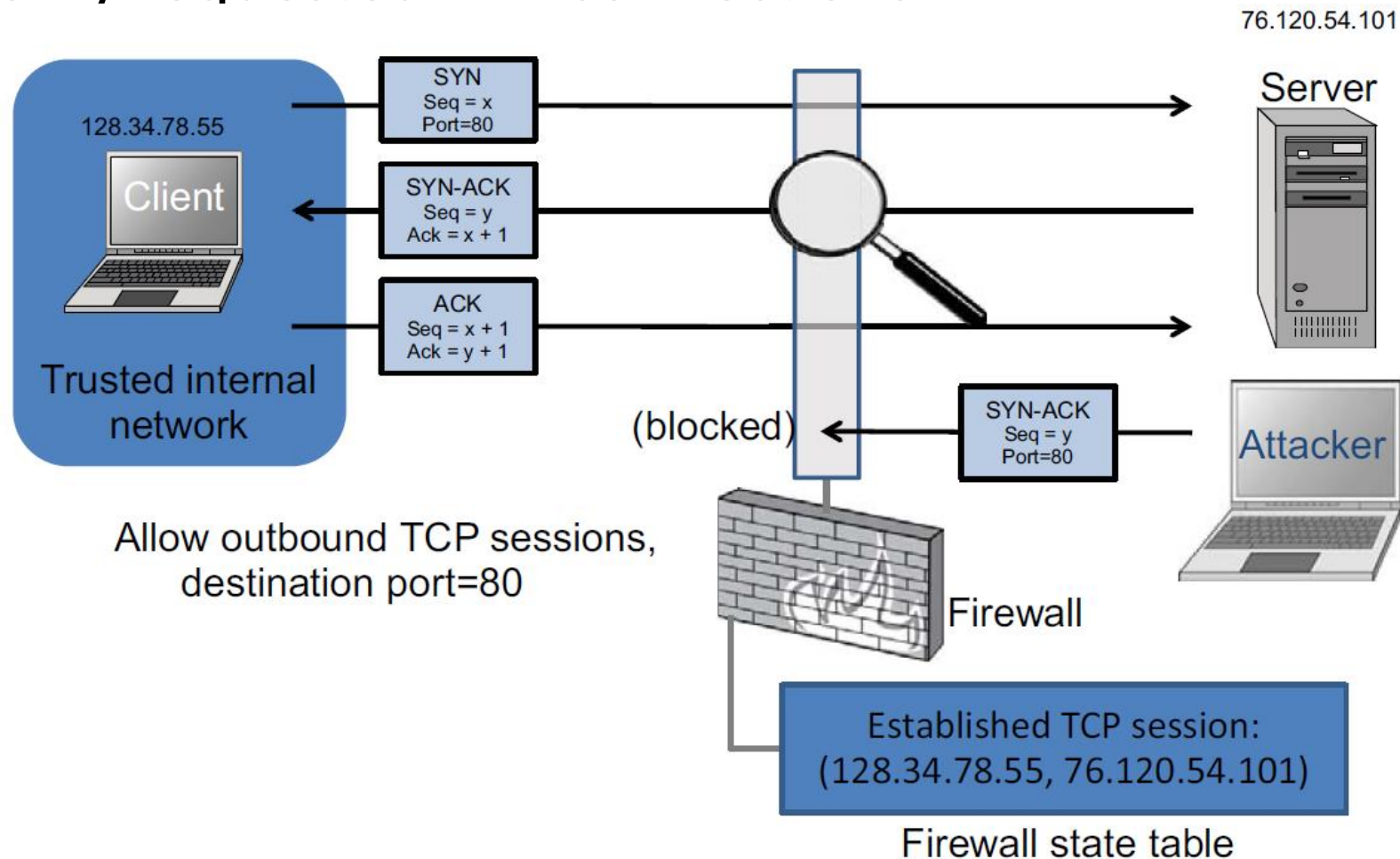
---

- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.



# Stateful Firewall Example

- Allow only requested TCP connections:



# Port scan

- An attacker is looking for applications listening on ports
- A single IP address (right) is contacting many ports (left) to see if any respond

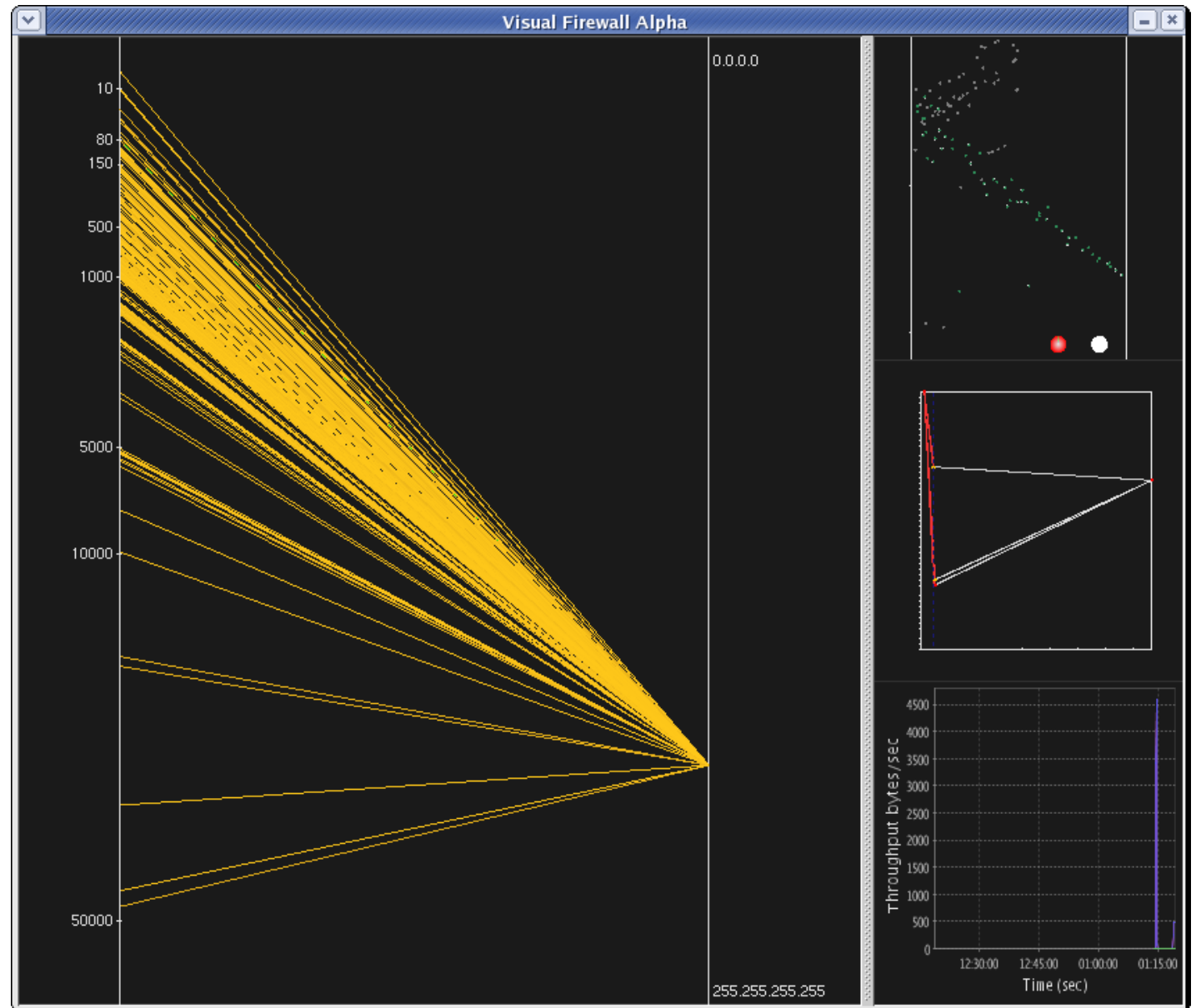



Image: <http://chrislee.dhs.org/projects/visualfirewall.html>



# Custom Firewall ruleset from a home router



```
root@ars-router: ~  
##### Service rules  
# OpenVPN  
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT  
  
# ssh - drop any IP that tries more than 10 connections per minute  
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DEFAULT --mask 255.255.255.255 --rsource  
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP  
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT  
  
# www - accept from LAN  
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT  
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT  
  
# DNS - accept from LAN  
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT  
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT  
  
# default drop because I'm awesome  
-A INPUT -j DROP  
  
##### forwarding ruleset
```



# Application layer firewall/proxy

---

- Simulates the (proper) effects of an application
- Effectively a **protective interceptor** that screens information at an application layer
- Allows an administrator to block certain application requests.
- For example:
  - Block all web traffic containing certain words (aka censorship)
  - Remove all macros from Microsoft Word files in email
  - Prevent anything that looks like a credit card number from leaving a database



# Personal firewalls

---

- Runs on the workstation that it protects (software)
- Provides basic protection, especially for home or mobile devices
- Any rootkit type software can disable the firewall



# Firewalls Pros and Cons

---

- **They do** prevent straightforward attacks and information leakages.
- **They can be circumvented**, and may have unintended consequences
- Increasing their effectiveness increases their operational cost substantially (overhead/configuration).
- May give false sense of security.
- **Bottom-line:** you have to have one but do not count on it for much.



# Network Address Translation (NAT)



Looking at the IP address of my laptop which is connected to the University WIFI.

```
Command Prompt

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::58d7:7d7d:b4c8:d930%10
    IPv4 Address. . . . . : 192.168.47.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6901:1d24:9977:fa5a%13
    IPv4 Address. . . . . : 192.168.248.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix  . : ed.ac.uk
    Link-local IPv6 Address . . . . . : fe80::44ed:201a:8a56:4c38%5
    IPv4 Address. . . . . : 172.20.145.155
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 172.20.159.254

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\marku>
```



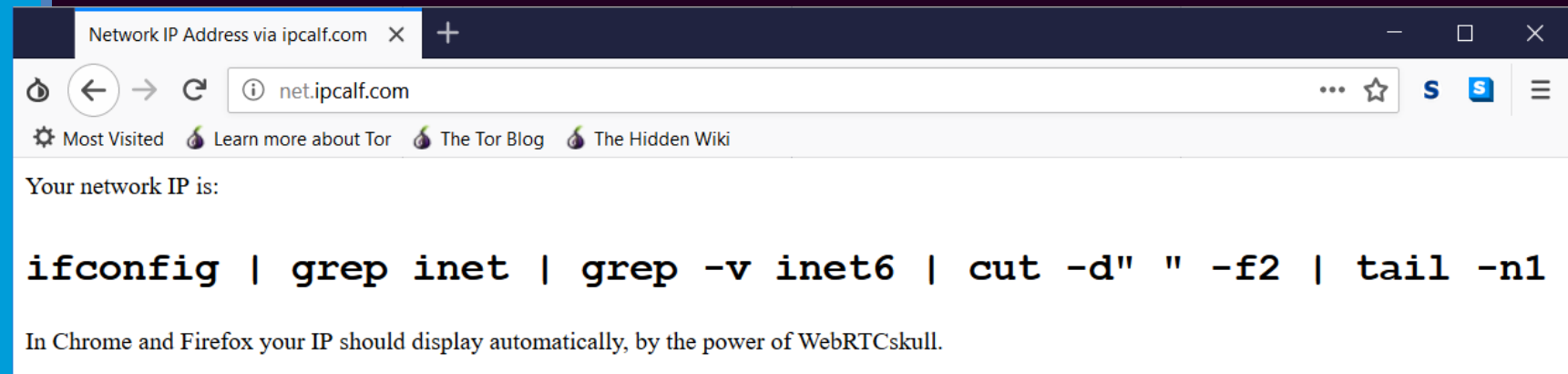
My computer  
as seen from a  
remote server

<http://www.hashemian.com/whoami/>

My IP  
previously  
showed as:  
172.20.106.96

What  
happened?

```
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.5
HTTP_CONNECTION: keep-alive
HTTP_COOKIE: __utma=145846189.271110778.1474893692.1474893692.1474893692.1; __utmc=.1474893692.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)|4893691768; PRUM_EPISODES=s=1474893750106&r=http%3A//www.hashemian.com/whoami/
HTTP_HOST: www.hashemian.com
HTTP_REFERER: https://www.google.co.uk/
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
REMOTE_ADDR: 192.41.131.255
REMOTE_PORT: 7535
REQUEST_METHOD: GET
REQUEST_TIME: 1474906336
REQUEST_URI: /whoami/
```



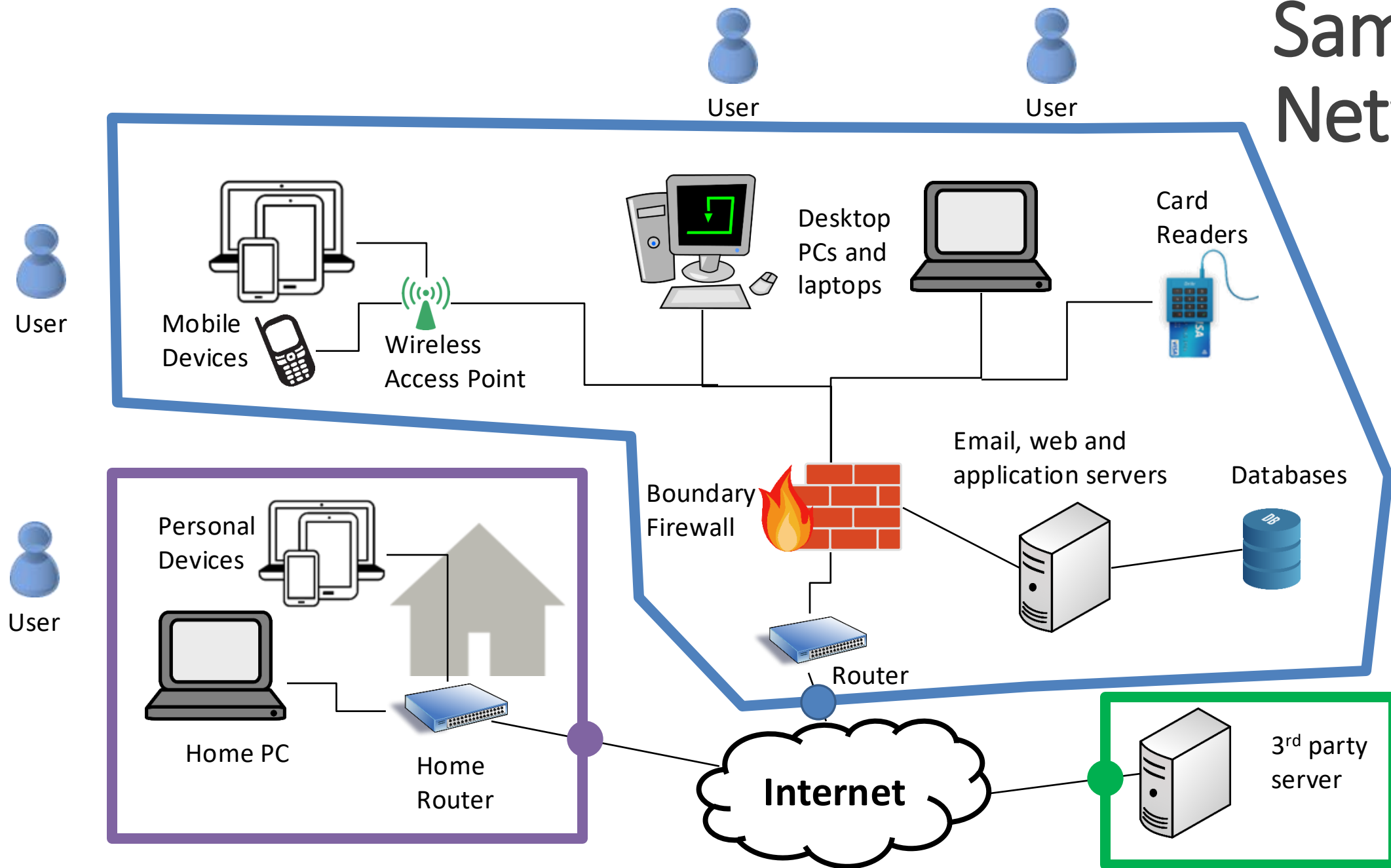
# IPv4 and address space exhaustion

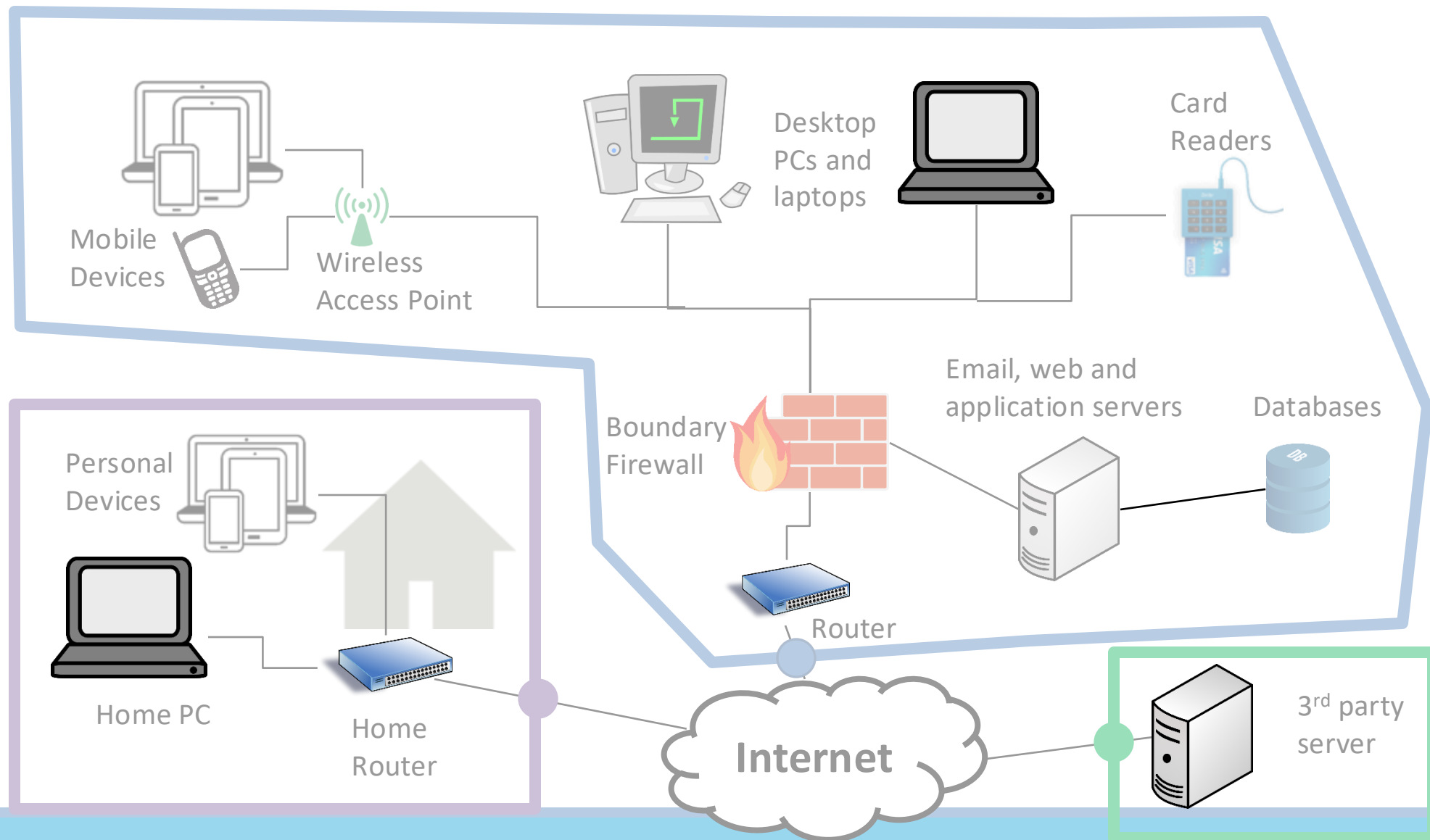
---

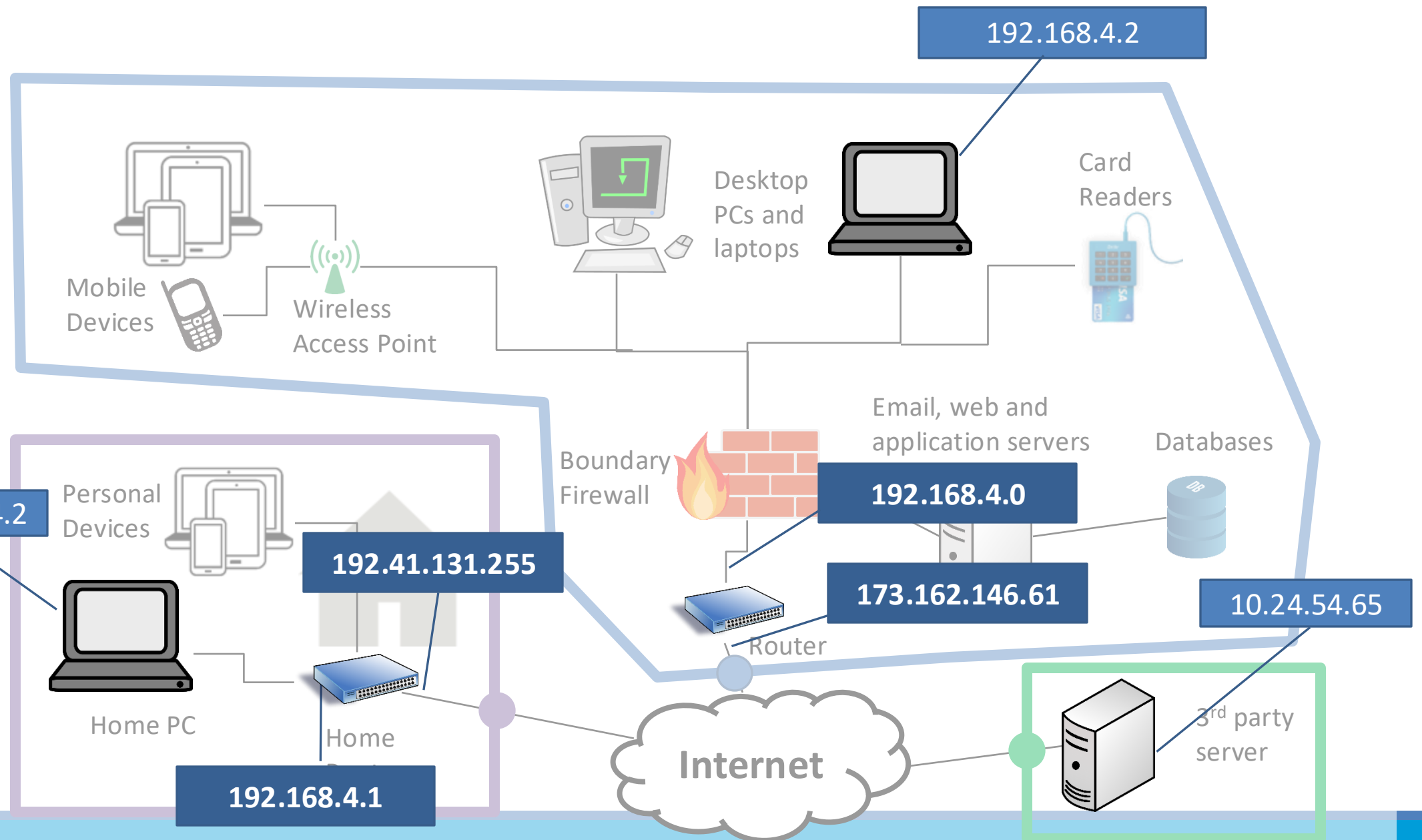
- Version 4 of the Internet Protocol
  - 192.168.2.6
- There are less than 4.3 billion IPv4 addresses available
- We do not have enough addresses for every device on the planet
- Answer: Network Address Translation
  - Internal IP different than external IP
  - Border router maps between its own IP and the internal ones
- Alternative Answer: IPv6?



# Sample Network







My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIFI.

```
Command Prompt

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::58d7:7d7d:b4c8:d930%10
    IPv4 Address. . . . . : 192.168.47.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6901:1d24:9977:fa5a%13
    IPv4 Address. . . . . : 192.168.248.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : ed.ac.uk
    Link-local IPv6 Address . . . . . : fe80::44ed:201a:8a56:4c38%5
    IPv4 Address. . . . . : 172.20.145.155
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 172.20.159.254

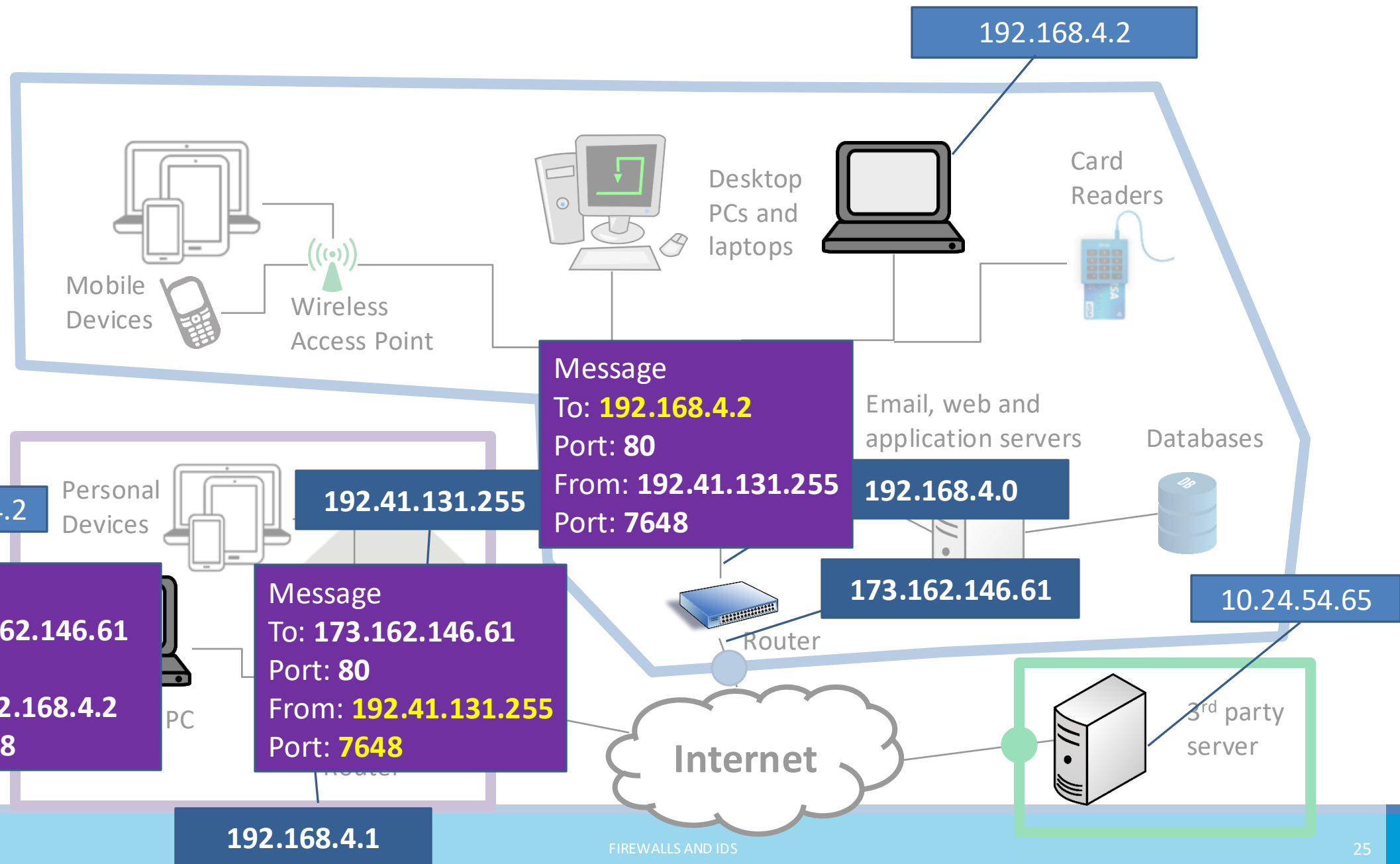
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\marku>
```







# Convenience vs security/privacy

## How Secure Are Wi-Fi Security Cameras?



CHRIS HOFFMAN [@chrisbhoffman](#)

JUNE 17, 2018, 6:40AM EDT



Everyone's seen the horror stories. Someone placed an Internet connected camera in their home and left it open to attack, allowing strangers to eavesdrop on their most private moments. Here's how to pick a camera that guarantees your privacy.

# Intrusion Detection Systems (IDS)



# Firewalls are preventative, IDS detects a potential incident in progress

---

- At some point you have to let some traffic into and out of your network (otherwise users get upset)
- Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves
- These cannot be prevented or anticipated in advance
- The next step is to identify that something bad is happening quickly so you can address it







# Possible Alarm Outcomes

---

- Alarms can be sounded (positive) or not (negative)

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	True Positive	False Positive
No Alarm Sounded	False Negative	True Negative



# Rule-Based Intrusion Detection

---

- Rules identify the types of actions that match certain known intrusion attack. Rule encode a **signature** for such an attack.
- Requires that admin anticipate attack patterns in advance
- Attacker may test attack on common signatures
- Impossible to detect a new type of attack
- High accuracy, low false positives



# Statistical Intrusion Detection

---

- Dynamically build a statistical model of acceptable or “normal” behavior and flag anything that does not match
- Admin does not need to anticipate potential attacks
- System needs time to warm up to new behavior
- Can detect new types of attacks
- Higher false positives, lower accuracy





# Base-Rate Fallacy

---

Suppose an IDS is 99% accurate, having a 1% chance of false positives or false negatives.

Suppose further...

- An intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Because of the success rate of the IDS, of the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative**.
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That is, roughly 99% of our alarms are false alarms.



# Number of alarms is a big problem

---

- In the **2013 Target breach** the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a liability



# Key take-aways

---

- Well configured Firewalls are helpful tools to defend against known attacks
- Network Address Translation allows traffic to flow from routable Internet addresses and private local area networks, but we have to be careful
- Intrusion detection systems may be able to detect malicious activity that the Firewall allows (due to usability reasons)
- A layered approach (Firewalls+IDS) is more resilient (but not perfect!)