Firewalls and Intrusion Detection

MARKULF KOHLWEISS COMPUTER SECURITY

Some slides adapted from those by Kami Vaniea, and Michael Goodrich

End-to-End Principle

Application-specific features

- should reside in the communicating end nodes of the network,
- rather than in intermediary nodes, such as routers, that exist to establish the network

Examples:

- reliability from unreliable parts
- end-to-end encryption and authentication

Counter examples:

- content distribution networks
- network address translation

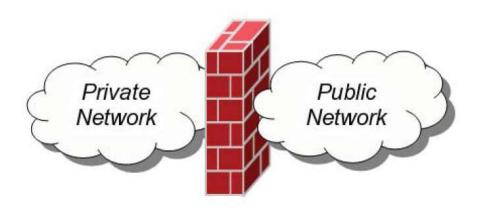


Today

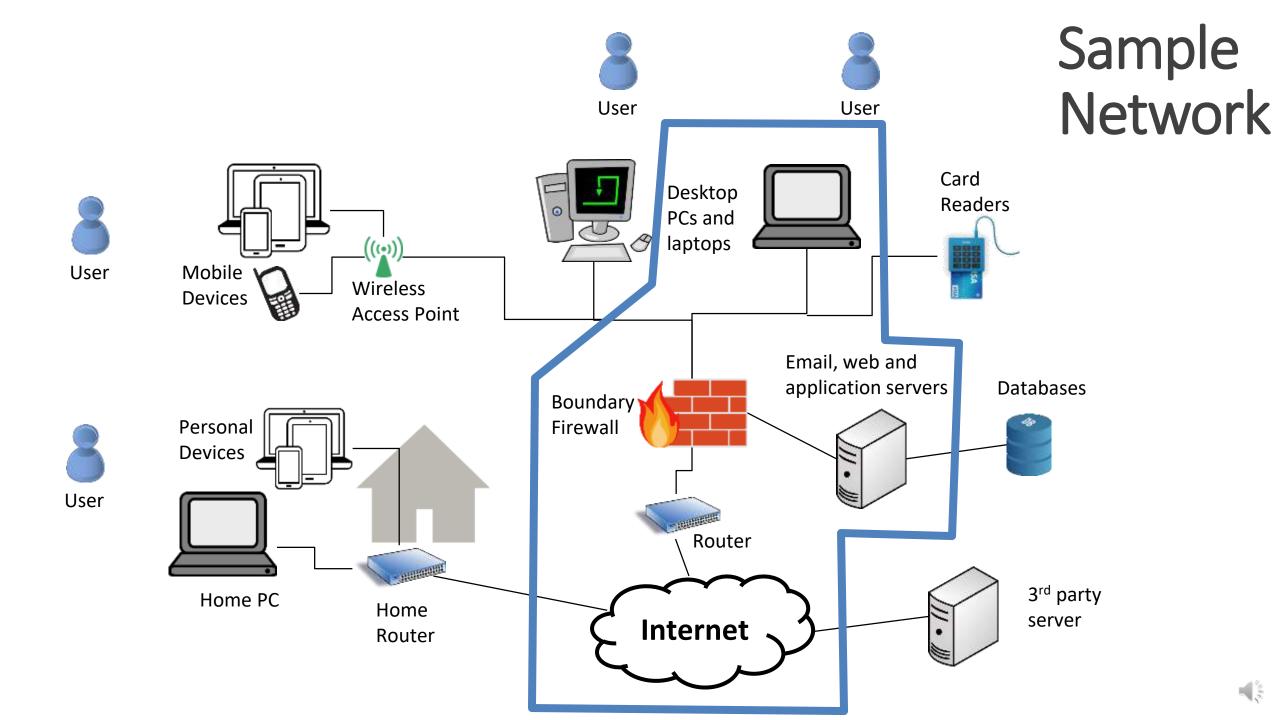
- Firewalls
- Network Address Translation (NAT)
- Intrusion Detection Systems (IDS)

Firewalls

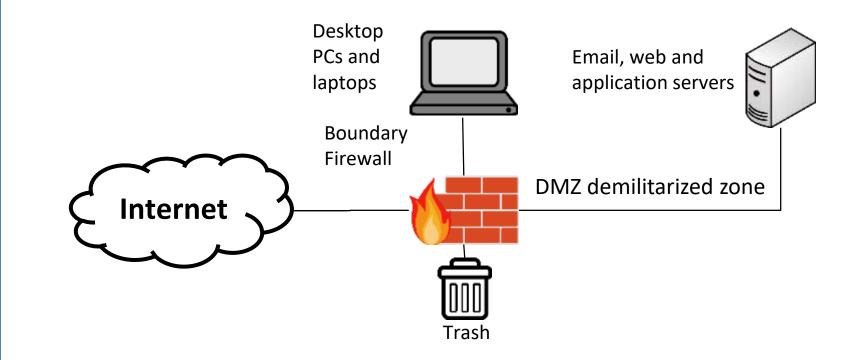
- A firewall is a security measures designed to prevent unauthorized electronic access to a networked computer system.
- Intuition: Similar to firewalls in building construction. Intent is to isolate one "network" or "compartment" from another.







- 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



Rule	Туре	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



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.

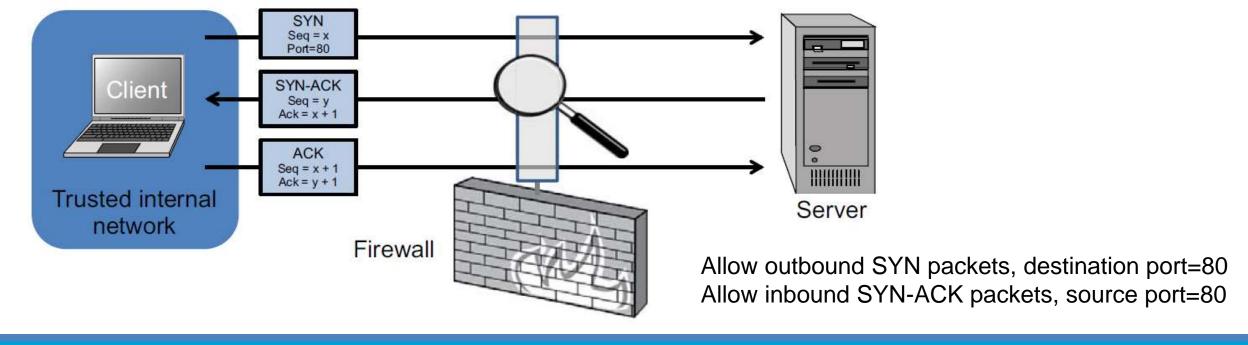
application layer

- 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, ...)

1

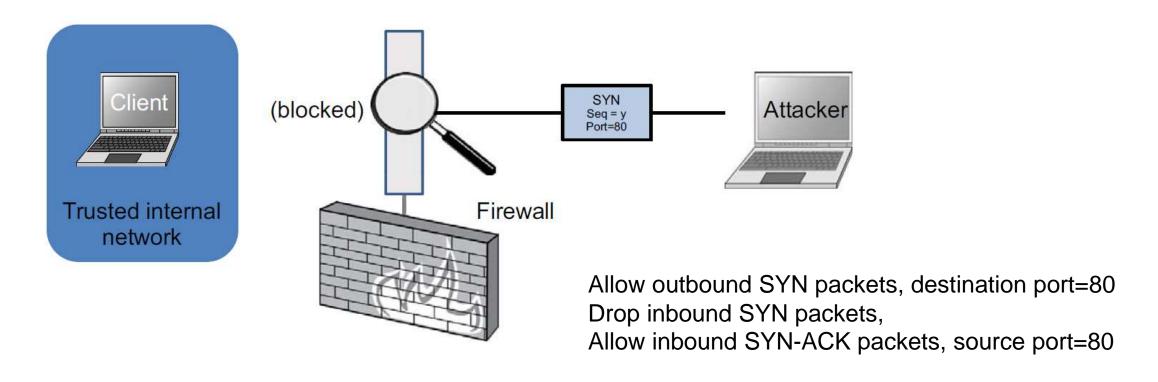
Stateless Firewalls

 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.



Stateless Restrictions

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



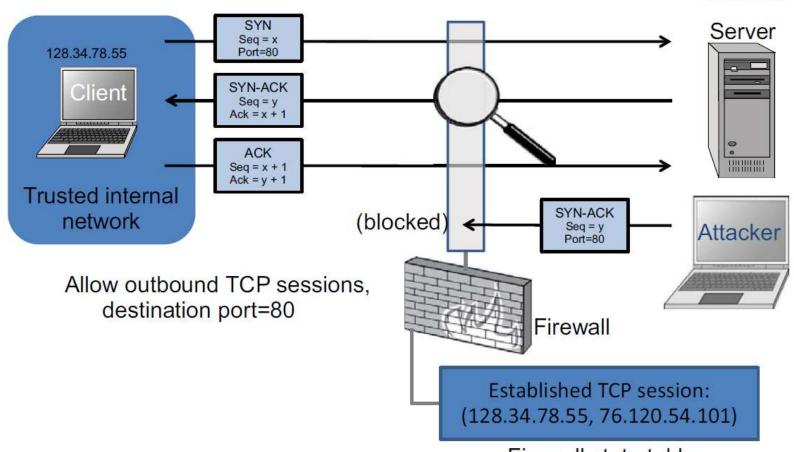
- 5

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:

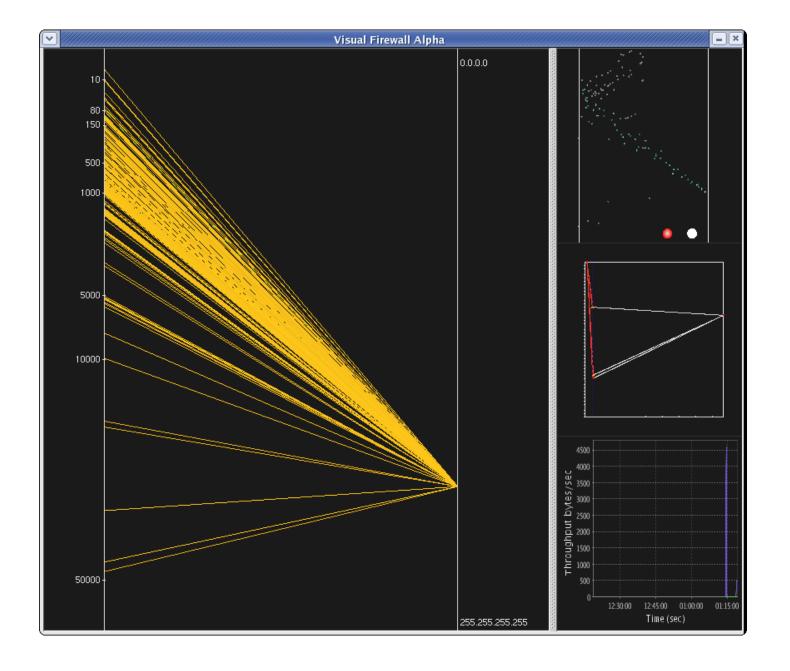


Firewall state table

76.120.54.101

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





Application layer firewall/proxy

- Simulates the (proper) effects of an application at OSI level 7
- Effectively a protective man-in-the-middle that screens information at an application layer (OSI 7)
- Allows an administrator to block certain application requests.
- For example:
 - Block all web traffic containing certain words
 - Remove all macros from Microsoft Word files in email
 - Prevent anything that looks like a credit card number from leaving a database

4/2

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



Think-pair-share

- Think quietly to yourself for 1 minute
- Pair and discuss with your neighbour for 3 minutes
- Share with the class group discussion

Think about the different types of firewalls.

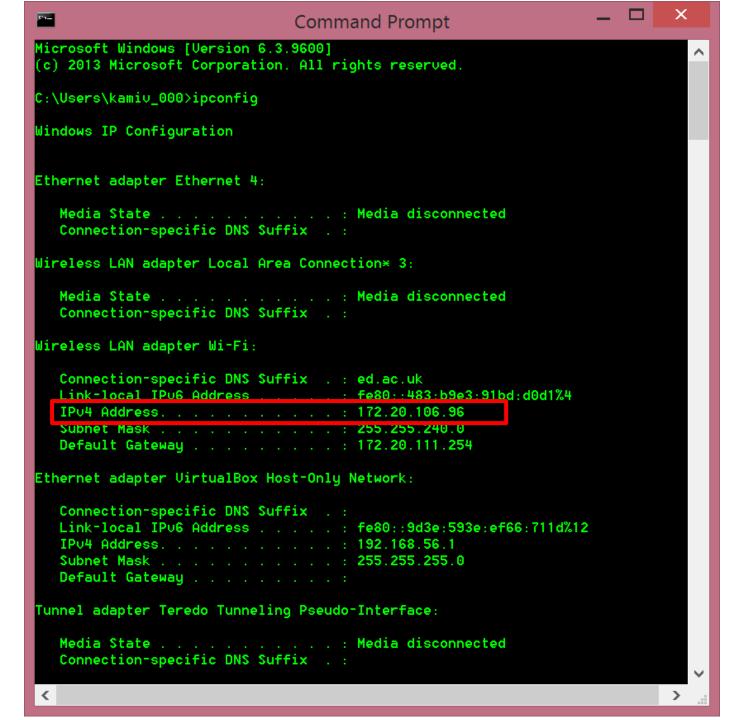
Do they violate the end-to-end principle?

Application-specific features should reside in the communicating end nodes of the network

Network Address Translation (NAT)



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





My computer as seen from a remote server

(http://www.hashemian.com/
whoami/)

My IP previously showed as: 172.20.106.96

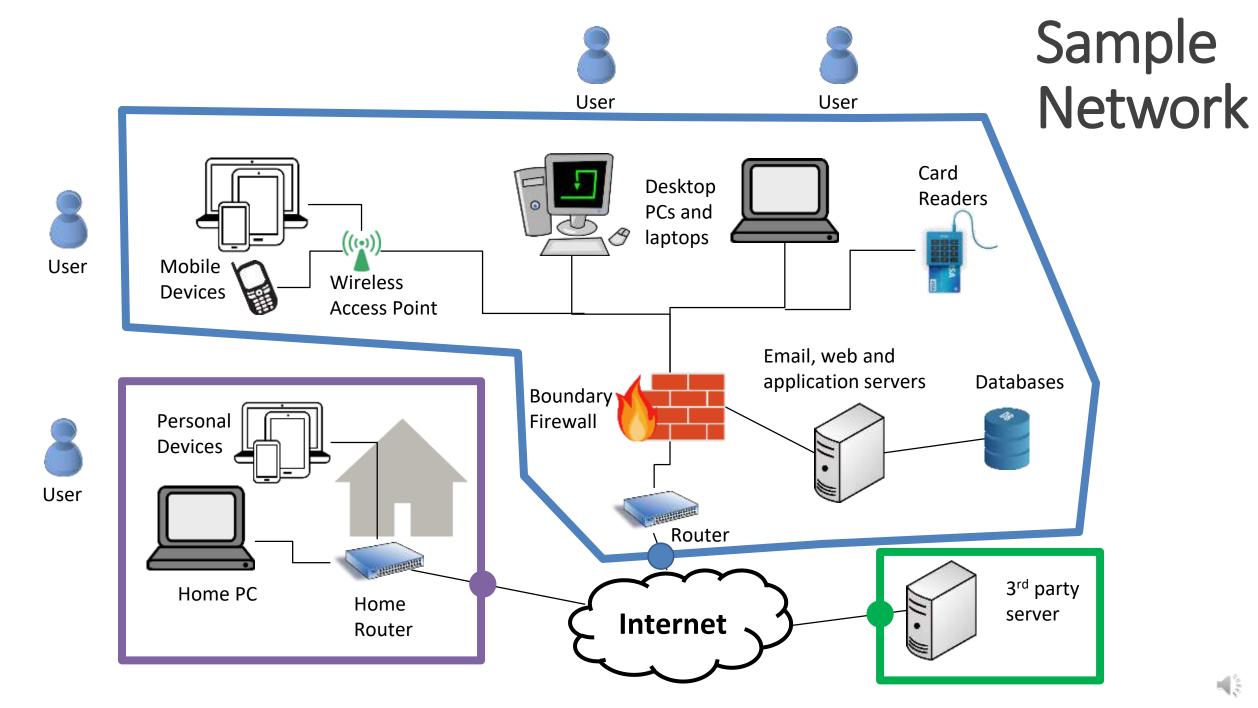
What happened?

```
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%20provide
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 Firefo
REMOTE ADDR: 192.41.131.255
REMOTE PORT: 7535
REQUEST METHOD: GET
REQUEST TIME: 1474906336
REQUEST_URI: /whoami/
SERVER ADDR: 173.162.146.61
SERVER_NAME: www.hashemian.com
SERVER PORT: 80
SERVER PROTOCOL: HTTP/1.1
SERVER SIGNATURE:
SERVER SOFTWARE: Apache
```

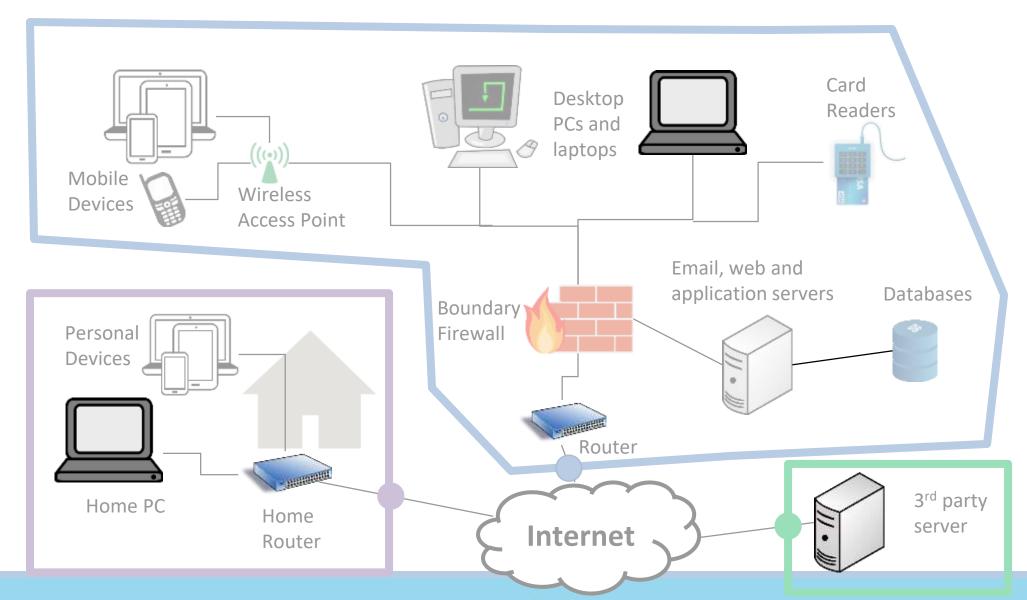
IPv4 and address space exhaustion

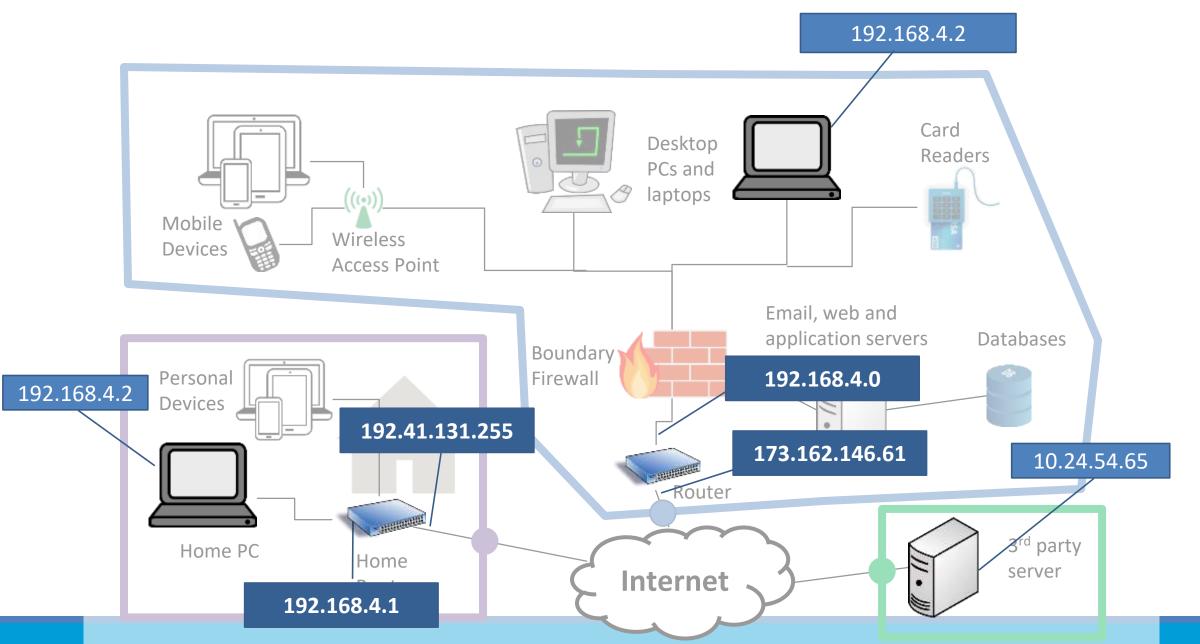
- Version 4 of the Internet Protocol
 - · 192.168.2.6
- There are less than 4.3 billion IPv4 addresses available
- We do not have enough addresses for every device on the planet
- Answer: Network Address Translation
 - Internal IP different than external IP
 - Border router maps between its own IP and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

4



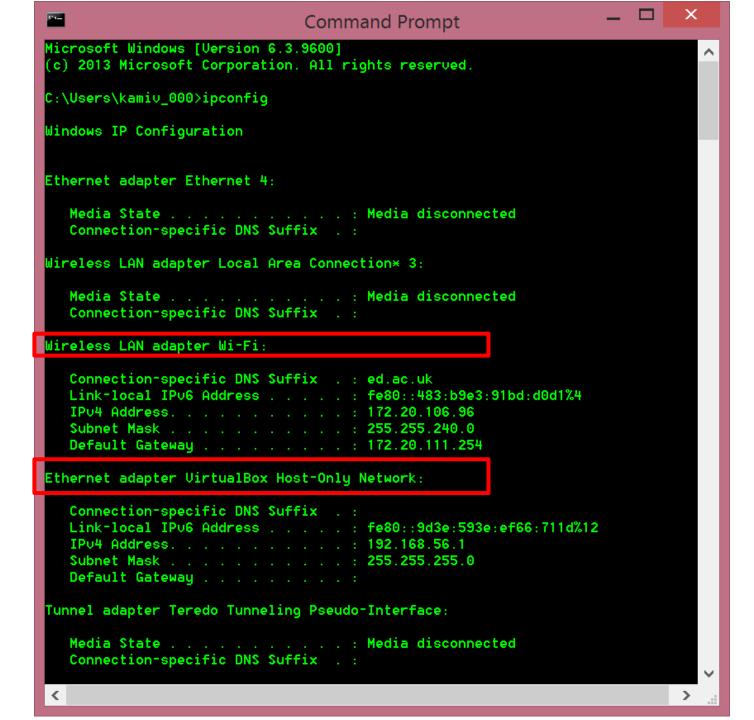




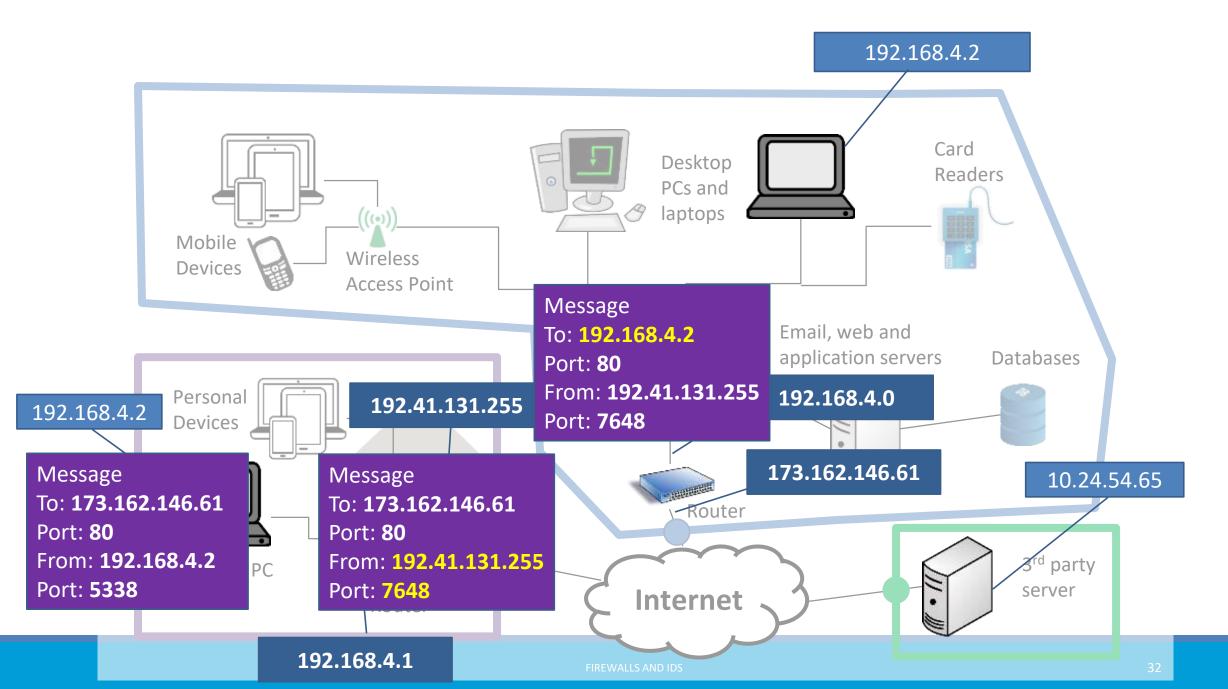




My laptop can have multiple IPs and bridge networks too. Here it shows IPs for both my VirtualBox and my WIFI.









Think-pair-share

 Internet of Things (IoT) security cameras commonly advertise that you have the ability to see the video feed from anywhere using their app

 What would they need to do to technically implement this?

 Advanced: How do you think they are actually accomplishing this?

https://www.youtube.com/watch?v=ISwB49vO0ys



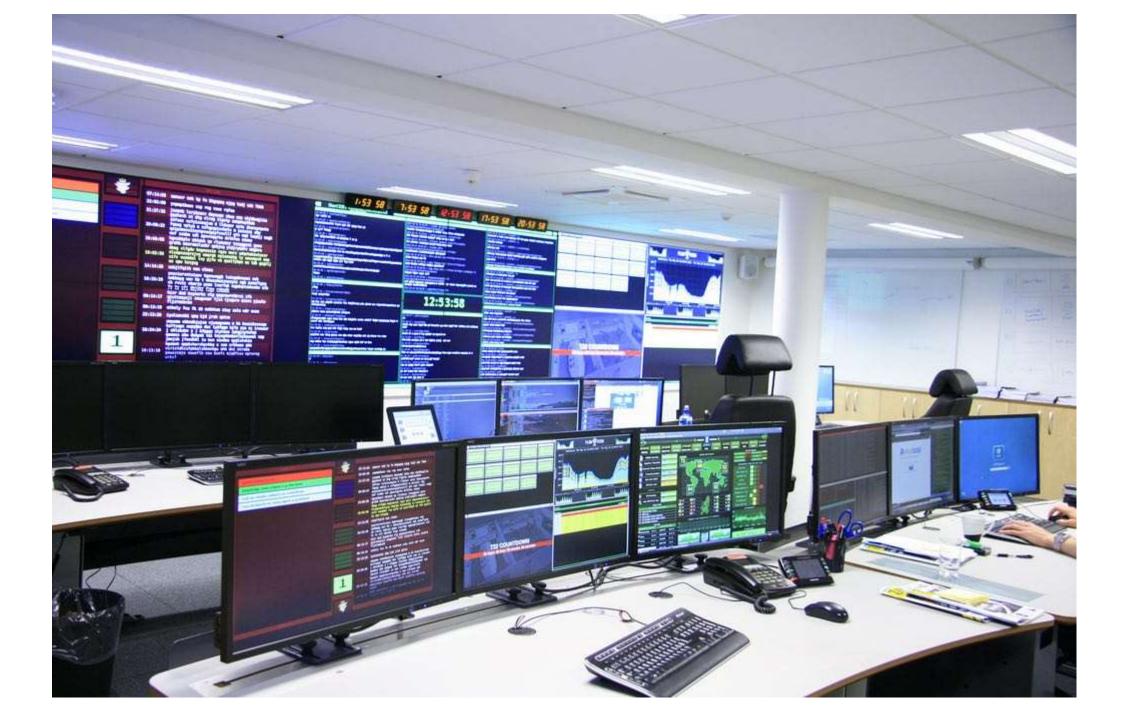
Intrusion Detection Systems (IDS)



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

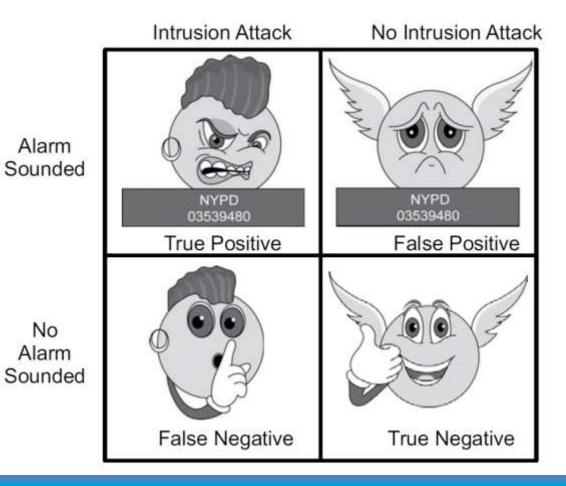






Possible Alarm Outcomes

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





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



Questions

Piazza: https://piazza.com/class/jqw6jfkkzns3l0

"Hard statistical data prove that emotional support directly impacts every metric of academic performance — and, as it turns out, every other aspect of our lives as well." Mark Greene



In-depth analysis of the Great Firewall of China

Chao Tang December 14, 2016

TCP Reset

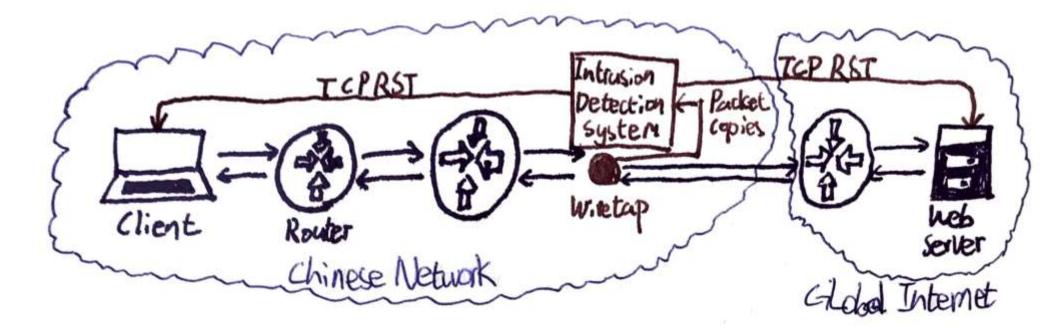


Figure-1: An illustration of TCP Reset

DNS Tampering

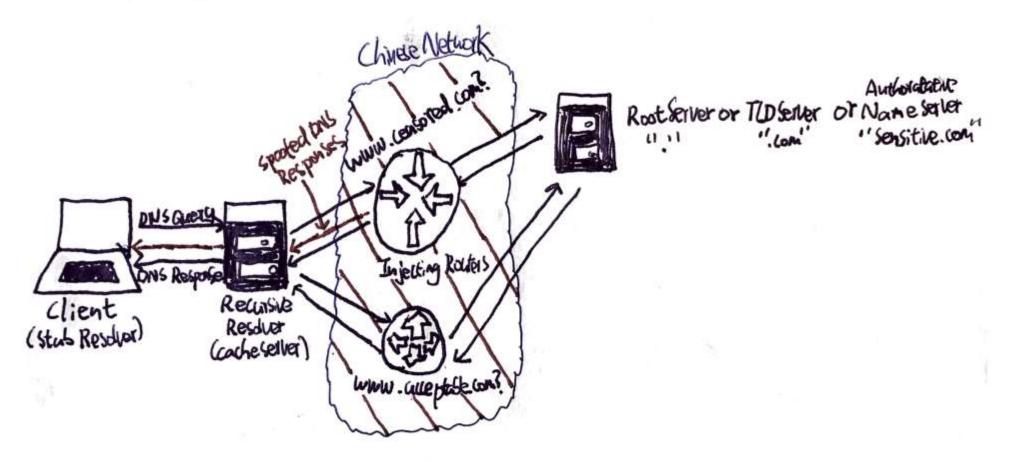


Figure-5: An illustration of DNS Tampering.