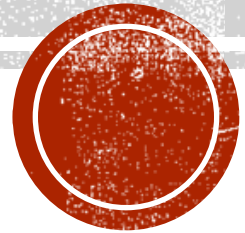
BORDER SECURITY

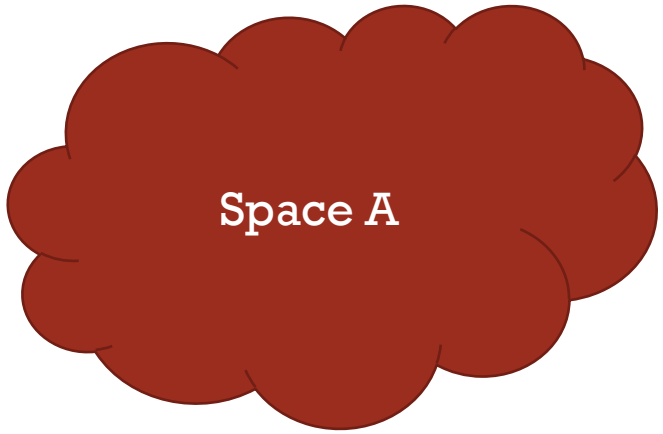
LAW 371

Fall 2022

Dr. Seth James Nielson

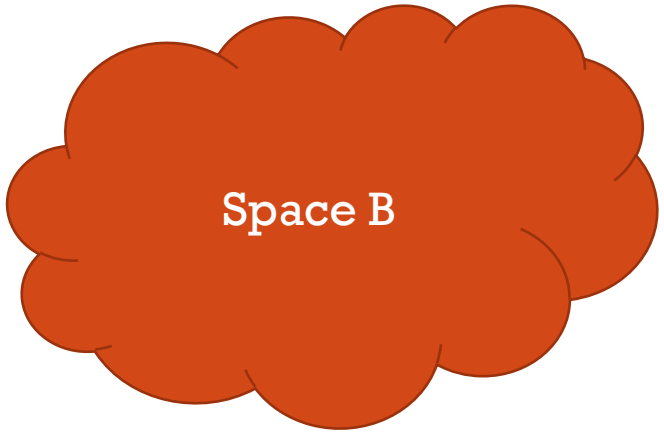


"SPACES"



"Space" is not a technical term.

I use it to represent the concept of separation



MACRO PHYSICAL SPACES

MICRO PHYSICAL SPACES

WHY DO WE SEPARATE PHYSICAL THINGS?

- ***CONTEXT***
- Countries have different
  - Social Models
  - Legal Frameworks
  - Rights and Responsibilities
- Binders, bins, and office "spaces"
  - Importance
  - Meaning

ACCESS

Most physical spaces try to control the flow
from one space to another

CYBER SPACES

- Often tied to a physical space and/or organization
  - All the people, equipment, data, etc. belonging to an entity
  - For example, a corporate network
- But there are far more conceptual spaces
  - Media piracy
  - Hacking communities
- Everything in-between

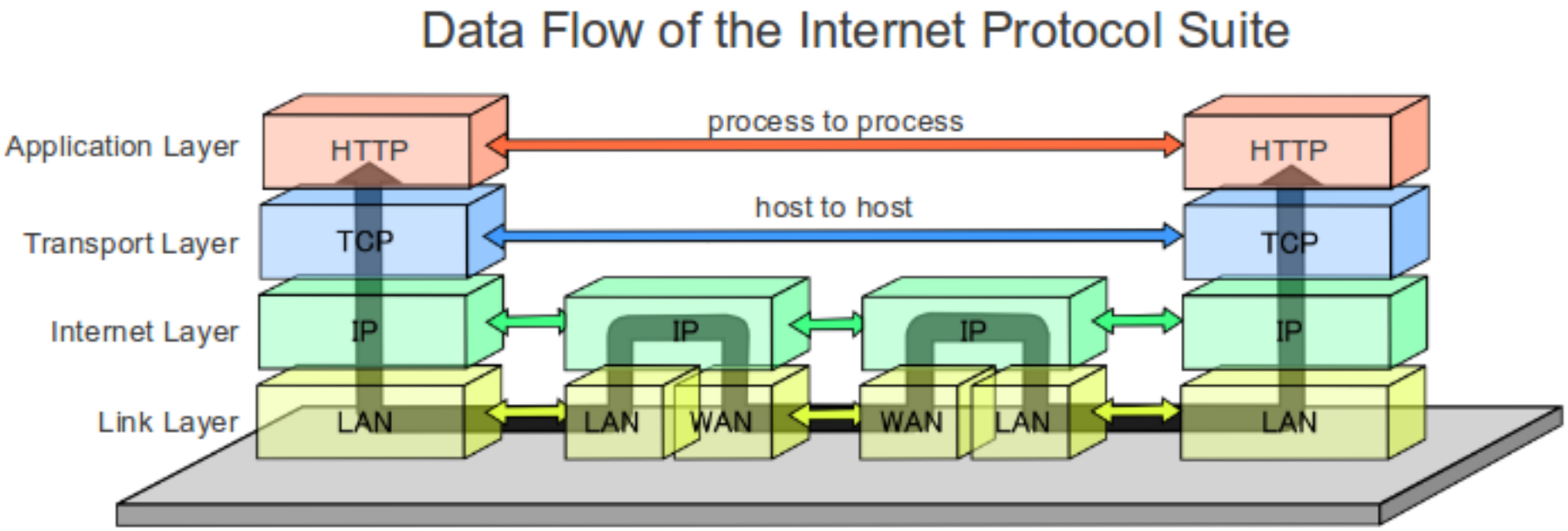
REVIEW: LOCAL AREA NETWORKS

- What is a LAN?
- Generally communicates ***WITHOUT ROUTING***
- This is why it is "local"

LAN'S AS NATURAL SPACES

- LAN's have *historically* created cyber spaces very naturally
- Typically tied to an entity, the LAN is
  - Hosted by the entity **in physical space**
  - Provides resources on behalf of the entity in cyber space
- Access controls are typically related to physical entity
  - Insiders have increased access to resources across the LAN
  - Outsiders have limited access to specific servers/resources

LAN'S CREATE "BORDERS" ON THE INTERNET

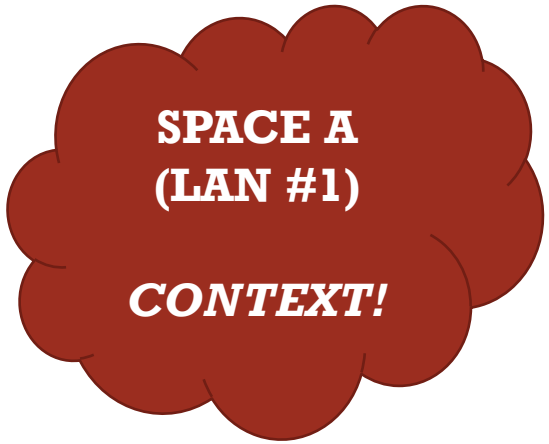


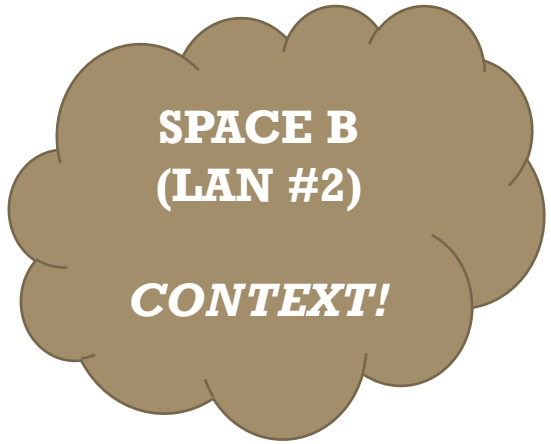
LAN #1 **ROUTER (Gateway)** **ROUTER (Gateway)** **LAN #2**

GATEWAYS: NATURAL BARRIERS

- Outside data can only get into a LAN via router
- We call the routers at the "edges" of a LAN ***gateways***
- Gateways are, therefore, ***natural chokepoints for data***

GATEWAYS: SPACE TRANSITION





CONTEXT IS EVERYTHING

- Security is all about ***context*** (REPEAT AFTER ME!)
- Security has no meaning without context
- What is secure in one context may not be in another
- Outside data is *assumed* to have a different context
- Reasonable and natural to examine data changing context

GATEWAYS: CONTEXT CHANGE

FIREWALL: GATEWAY SECURITY

- What is a "firewall"?
- Informally: any security-enforcement on data transit
- (most commonly at the gateway)

FIREWALL MARKETING

- **Juniper**: "control over applications, users, and content to stop advanced cyber-threats"
- **PAN**: "Instantly find and stop attacks with a fully automated platform"
- **Cisco**: "Prevent breaches, get deep visibility to detect and stop threats fast"

IGNORE MARKETING. THINK ***ENGINEERING***

- Ross Anderson's framework from ***Security Engineering***
  - Policy: ***WHAT*** you're supposed to achieve
  - Mechanism: ***HOW*** you're supposed to achieve it
  - Assurance: ***RELIABILITY*** of the mechanism
  - Incentives: ***MOTIVES*** of defenders and attackers

CORE CONCEPTS: *POLICY AND MECHANISM*

- This is not a security engineering class
- But we will use it to help us frame how we look at security
- PAY SPECIAL ATTENTION TO ***POLICY*** vs. ***MECHANISM***
  - Policy is WHAT you want
  - Mechanism is HOW you do it

FIREWALLS: POLICY AND MECHANISM

- Firewalls are MECHANISMS for enforcing certain network security POLICIES
  - Borders are natural places to ***want*** a policy
  - Borders are also an easy place to ***enforce*** some policies
  - BUT DON'T CONFUSE THE TWO!

"SECURITY" IS A MEANINGLESS WORD

- Firewalls, like other mechanisms, don't "create security"
- Consider the marketing descriptions
  - What is a "threat"?
  - What does it mean to "block"?
  - What is an "attack"?
- How would you even evaluate these claims?

ENFORCING POLICY

- Firewalls are ONLY useful to the extent they enforce policy
- Corollary: Policies come BEFORE firewalls
- What security policies might you like to have?
- How well do firewall enforce these?

SAMPLE POLICIES

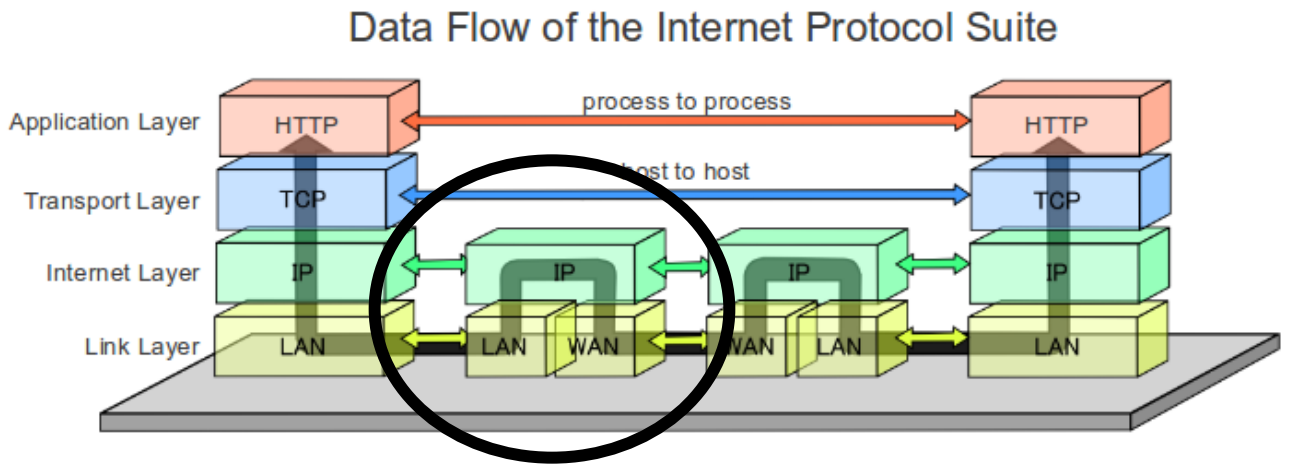
- Policy #1: Only authorized software can enter the network
- Policy #2: Only authorized external network access
- Policy #3: Only authorized published resources
- Policy #4: Authorized resources remain available

- NOTE:
  - External access means LAN user connecting to Internet
  - Published resources means Internet connecting to LAN

EARLY FIREWALLS: LAYER-3 MECHANISMS

- The first firewalls were LAYER 3 (IP level)
- Could only block bad IP addresses!
- Layer-3 filtering can only indirectly enforce
  - Policy #1 by blocking access to ***probably*** dangerous computers
  - Policy #2 by blocking outbound requests to unauthorized IP's
  - Policy #3 by blocking inbound requests to unauthorized servers
  - (Maybe some Policy #4?)

HOW DOES LAYER-3 ENFORCEMENT WORK?



Router/Firewall
-> Has to inspect the IP packet for routing
-> Will drop packets from "bad" addresses

LAYER-4 FIREWALL (PACKET FILTER ONLY)

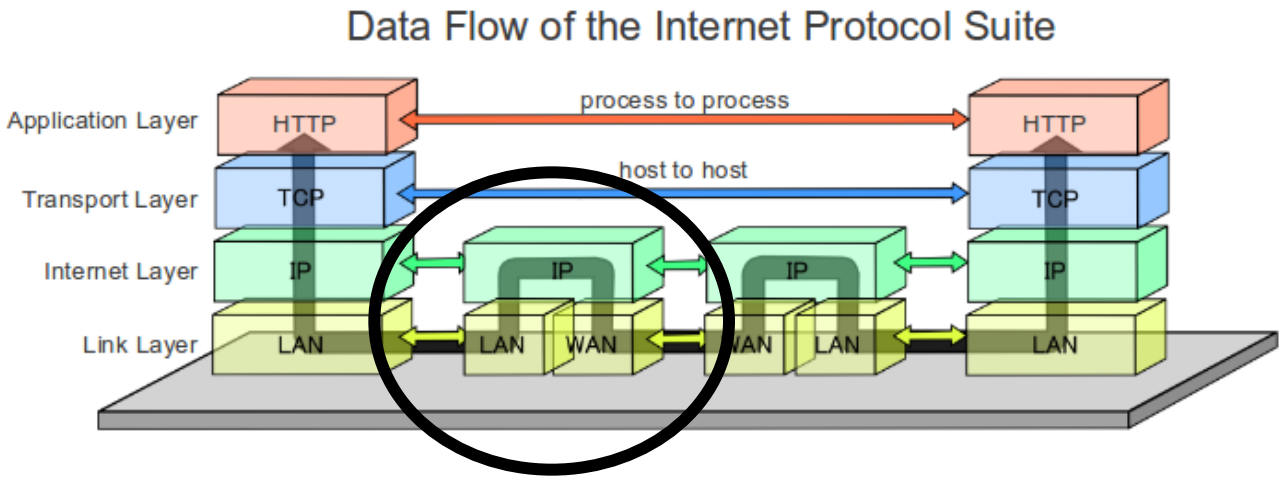
- People quickly realized that IP-layer was weak enforcement
- Examining TCP packets made enforcement better
  - TCP ports ***typically*** represented a specific service
- Policy enforcement mechanism improvements:
  - Policy #2 by blocking access to unauthorized outbound *ports*
  - Policy #3 by blocking access to unauthorized inbound ports

LAYER-4 FIREWALL (STATEFUL)

- Layer-4 packets also reveal *connection state*
- Some malicious packets violate TCP rules, for example
- Layer-4 firewalls could also keep track of TCP sessions
- Better enforcement of policy #4
  - Block malicious network traffic

LAYER-4 STILL LAYER-3 ROUTING

- Important.
- Just because a router is doing L3 routing doesn't mean it cant look at L4 data



Router/Firewall can examine ***any*** data, not just data used for routing

L7 FIREWALLS

- L7 firewalls examine application data
  - Specifically look at data, and not just headers!
  - Can "reassemble" data from more than one packet
- Even more "stateful"

EARLY MOTIVATIONS FOR L7

- Application firewalls go back to 1991!!
- Idea: Firewalls should ***understand*** application traffic.
- Example: File Transfer Protocol
  - Scan FTP data for the logged-in user
  - Scan FTP data for operations (upload/download)
  - Control which users can upload or download
  - Fine-grained application controls

MODERN MOTIVATION FOR L7

- In the past decades, need for L7 scanning has increased
- L3/L4 enforcement is rough guess (e.g., based on IP/port)
- What stops an attacker from using a different port number?
- L7 scanning can block web traffic even on different port
- Can also scan for viruses, malicious data
- (Better for all 4 policies!!!)

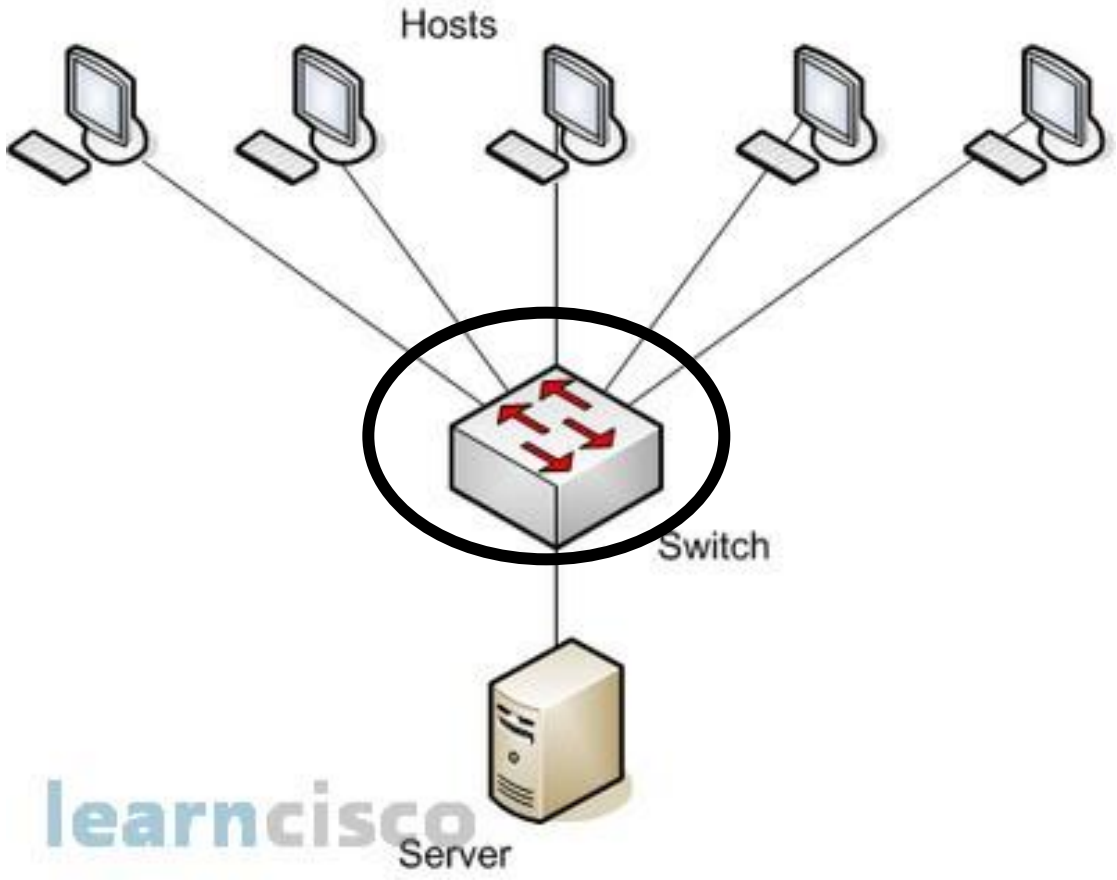
TRACKING USERS

- Since the 90's, firewalls also supported their own services
- Users could log-in to the firewall
- The logging-in process could map a
  - user-name to an IP address (computer)
  - Or even a special connection like VPN

L7 POLICY ENFORCEMENT

- User + Application Scanning even more granular
- Resource access can now be user specific
  - User X can connect to specific external website

YOU CAN ALSO HAVE AN L2 FIREWALL



Firewalls can go here too!

In this case, L2 refers to the routing, not the inspection!

LAYER 2 FIREWALLS

- But this is REALLY confusing
- Has nothing to do with layer used for scanning
- Just refers to scanning in a SWITCH instead of a ROUTER
- Have some neat defensive properties
  - If only a switch, ***HAS NO IP ADDRESS!!! HARDER TO ATTACK!!!***
  - Called "bump in the wire"

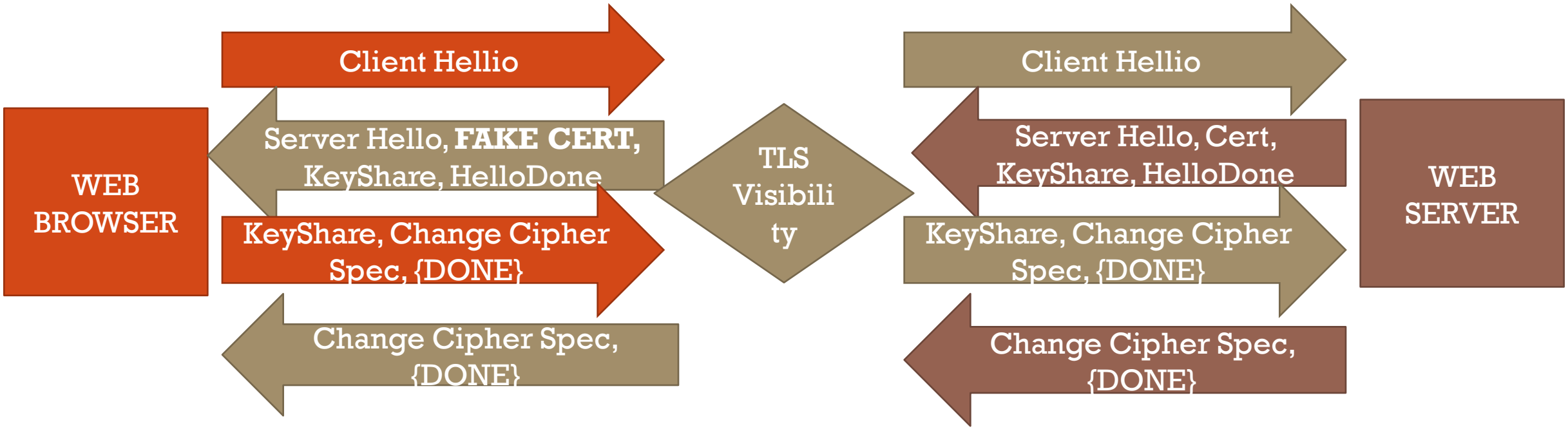
TUNNELS

- In the arms race, bad actors wrap one kind of traffic in another
- Unsurprisingly, HTTP is popular
- Modern firewalls can unpack the tunnel to see what's inside.
- One exception: encrypted tunnels (TLS/SSH)
- Can't see inside without "visibility"

TLS VISIBILITY

- Typically, client MUST have a new root CA installed
- Root CA is a self-signed certificate from the firewall
- Firewall can now generate ANY cert!!!

TLS VISIBILITY HANDSHAKE VISUALIZATION



IDS: MITIGATION AND FUTURE PREVENTION

- IDS stands for Intrusion Detection System
- IPS is Intrusion Prevention System
- IDS is far more common because IPS is just too hard (FP/FN)
- IDS assumes the attacker has already won
  - The attacker has already succeeded in his objective and left (forensics)
  - The attacker is in the system, but moving to a higher target (mitigation)

SIGNS OF BAD BEHAVIOR

- Anomalies: unusual network traffic
  - Port scanning (recon)
  - Unusually large data transmissions (buffer overflow, etc)
  - Unexpected traffic between machines
- Surprisingly, this is still very much signature based
- Many attempts to do statistics modeling but usually too noisy

IDS TYPES

- Network Based IDS (NIDS)
  - Monitor traffic on the network (often using the gateways/routers)
- Host Based IDS (HIDS)
  - Monitor traffic received at a host, and the effect thereof
  - Sometimes helpful in simply monitoring the encrypted traffic
- Hybrid systems
  - Deploy host components and network components
  - Report all data back to a central server/dashboard

HONEYPOTS

- An interesting IDS component
- Create a fake system to draw attacker attention
- Introduces components whose entire operation is an anomaly

TYPES OF HONEYPOTS

- Low Interaction – port only, record traffic
  - Purpose: logging
- Medium Interaction – simulated/emulated service
  - Purpose: delay/confuse
- High Interaction – real services on real computers with real OS
  - Purpose: maximum analysis of attacker behavior
- Honeynet – multiple honeypots together on fake network
- Specialized variants:
  - Malware Honeypots
  - Spam Honeypots

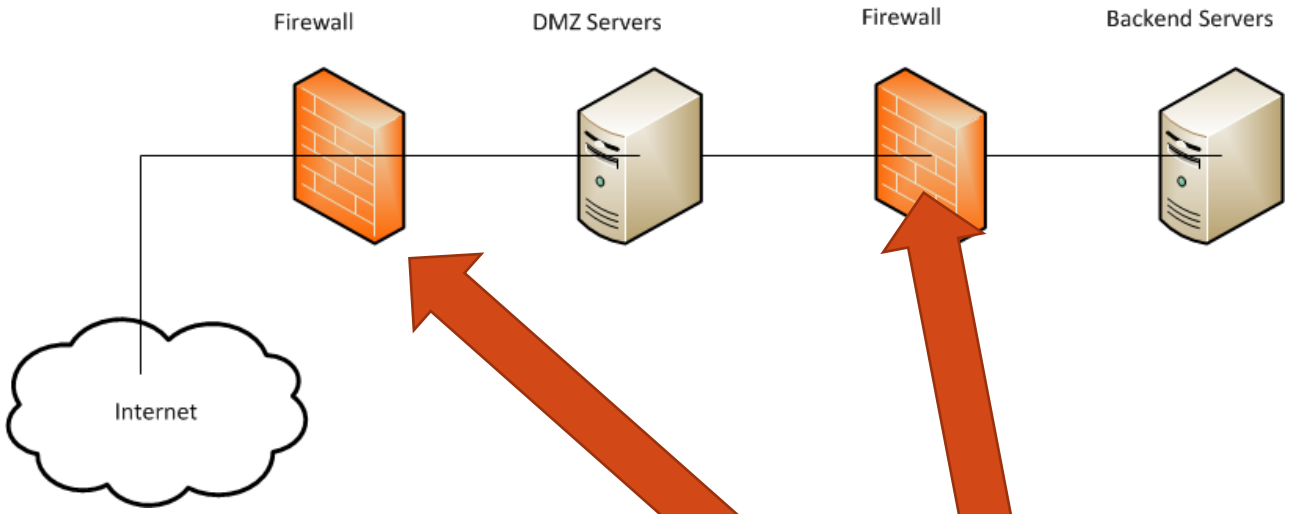
DEPLOYING HONEYPOTS

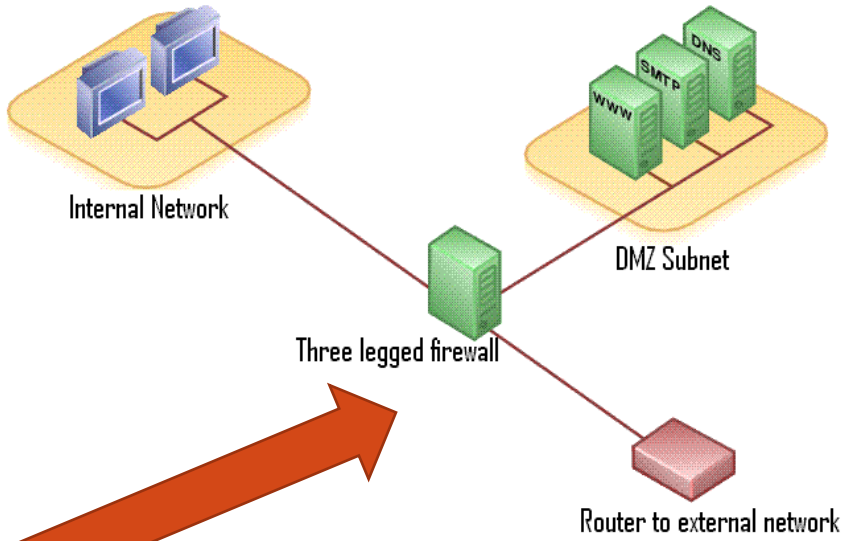
- Now part of larger "Enterprise Deception Operations"
- Entire firms dedicated to setting up fake systems
- Shockingly useful these days… why?
  - Use up attacker time
  - More time to detect attacker
  - More likely to feed false information to attacker

ALL-IN-ONE

- Most "enterprise" firewalls for sale include extras like IDS
- Generally easier to have it all in one

NETWORK ARCHITECTURE: DMZ





POLICY ENFORCEMENT

THE FUTURE

- The future? ***ZERO TRUST NETWORKS***
- Many say that the "Firewall is Dead", "DMZ's are Dead", etc
- I doubt that they die… will probably evolve?