BORDER SECURITY

EN.600.444/644

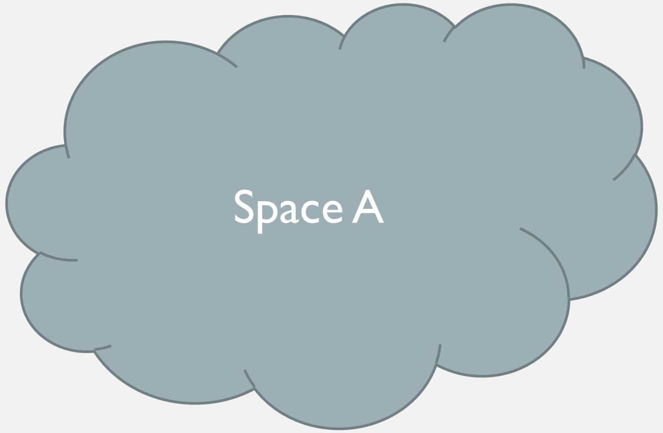
Spring 2021

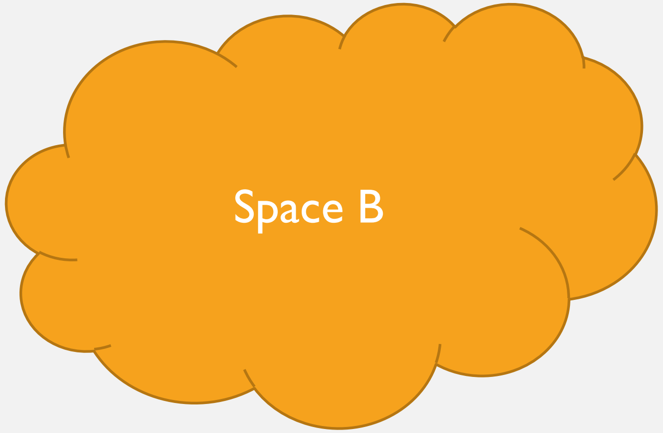
Dr. Seth James Nielson

“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

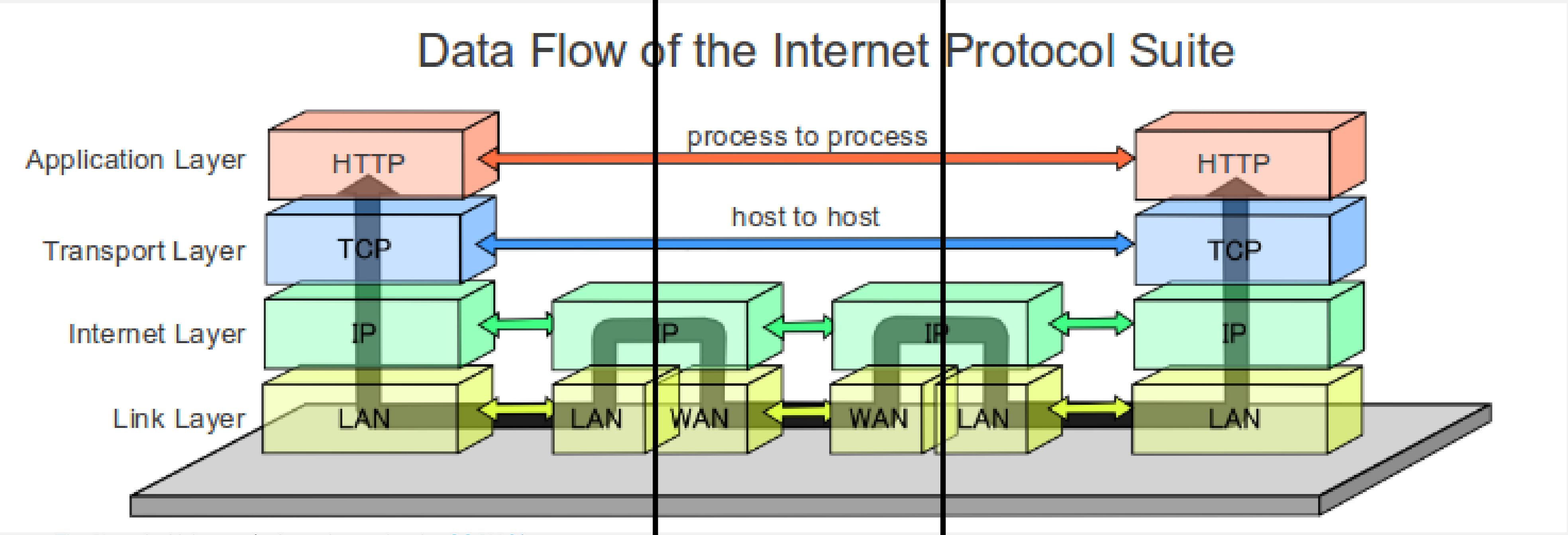
CYBER SPACES

- 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 inbetween

LAN’S AS NATURAL SPACES

- LAN’s have *historically* creates 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 is typically limited to individuals with physical relationships to the entity
  - Insiders typically have increased access to resources across the LAN
  - Outsiders typically have limited access to published resources on specific servers

LAN'S CREATE "BORDERS" ON THE INTERNET



ROUTER (Gateway)

ROUTER (Gateway)

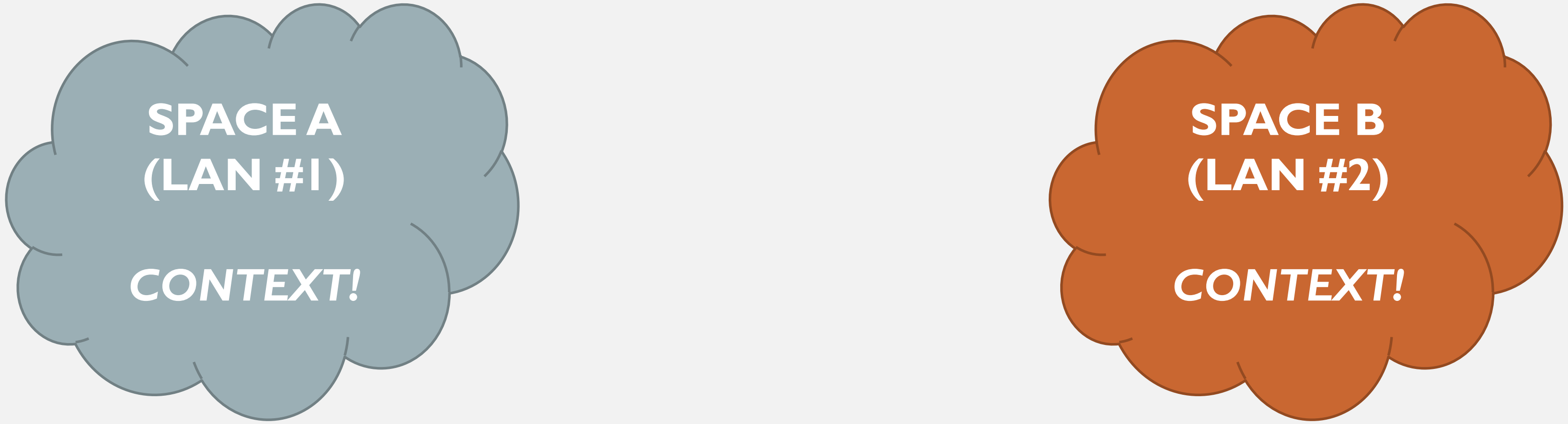
LAN #1

LAN #2

GATEWAYS: NATURAL BARRIERS

- 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



SPACE A
(LAN #1)

CONTEXT!

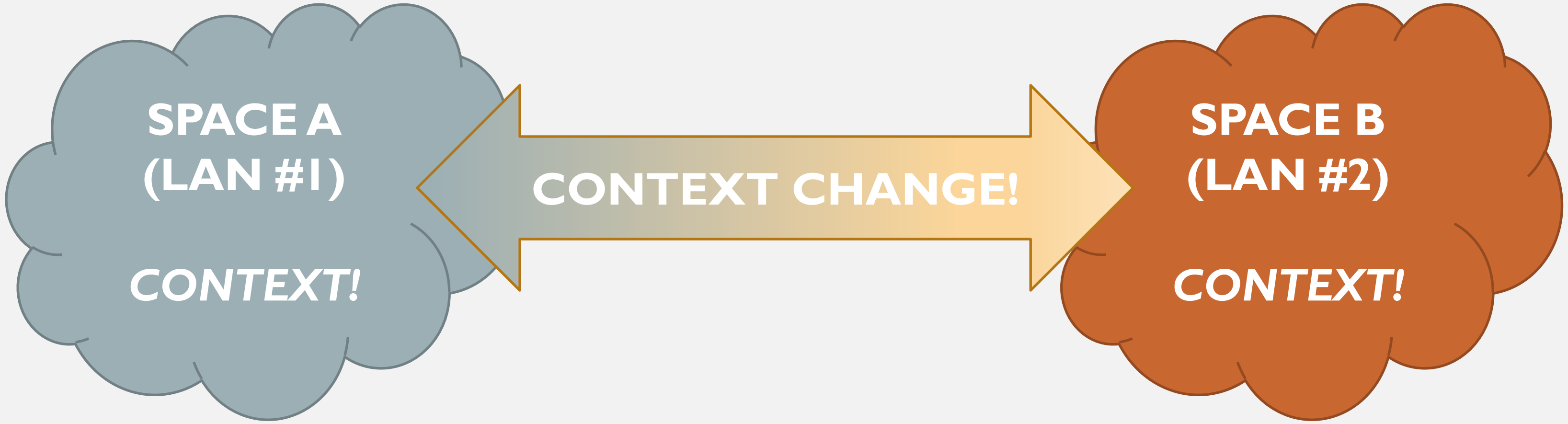
SPACE B
(LAN #2)

CONTEXT!

CONTEXT IS EVERYTHING

- Security is all about ***context*** (REPEAT AFTER ME!)
- Security has no meaning without context
- What is secure within one context may not be within another
- Data on different networks is *assumed* to have a different contexts
- It is reasonable and natural to examine data transitioning context

GATEWAYS: CONTEXT CHANGE



SPACE A
(LAN #1)

CONTEXT!

CONTEXT CHANGE!

SPACE B
(LAN #2)

CONTEXT!

FIREWALL: GATEWAY SECURITY

- What is a “firewall”?
- Informally, it’s security within a network connector, such as a gateway

FIREWALL MARKETING

- If you read marketing, it’s Super Man.
  - 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 proposed a framework for ***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
- Most “Policy” you see elsewhere, including CISSP, certifications, is different

EXAMPLE: TLS

- What is the ***POLICY?***
  - Authentication: a party can claim an identity ONLY if they're authorized to do so
  - Confidentiality: only authorized parties can READ the communications
- What is the ***MECHANISM?***
  - Authentication is enforced by certificates, signatures, and trusted authorities
  - Confidentiality is enforced by encryption
- ENCRYPTION IS MECHANISM NOT POLICY

FIREWALLS:
POLICY AND MECHANISM

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

“SECURITY” IS A MEANINGLESS WORD

- Firewalls, like every other mechanism, don’t “create security”
- Consider the marketing descriptions
    - What is a “threat”?
    - What does it mean to “block”?
    - What is an “attack”?
- As a security professional, how would you even evaluate these claims?

ENFORCING POLICY

- Firewalls are ONLY useful to the extent they can enforce a policy
- Corollary: Policies come BEFORE firewalls
- What security policies might you like to have?
  - Example 1: No malware can enter the network
  - Example 2: No unauthorized external network services
  - Example 3: External network services accessible only by authorized users
- Once you have a policy, you can start looking for enforcement mechanisms.

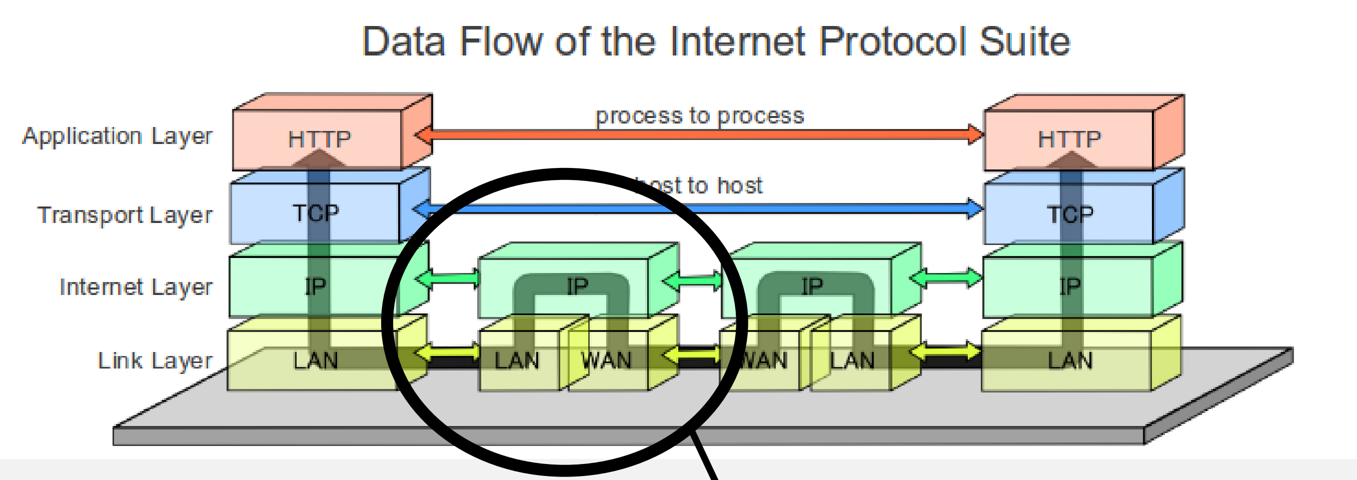
COMMON POLICIES: ACCESS CONTROL

- Policy #1: Only authorized LAN services are accessible outside the LAN
- Policy #2: Only authorized users from outside the LAN can access LAN resources
- Policy #3: Only authorized users on the LAN can access authorized services outside the LAN

EARLY FIREWALLS: LAYER-3 MECHANISMS

- The first firewalls were LAYER 3 (IP level)
- Layer-3 filtering can *partially* enforce all three policies:
  - Policy #1 by blocking access to computers without authorized services
  - Policy #2 by blocking access from computers without authorized IP's
  - Policy #3 by blocking outbound requests to unauthorized IP's

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)

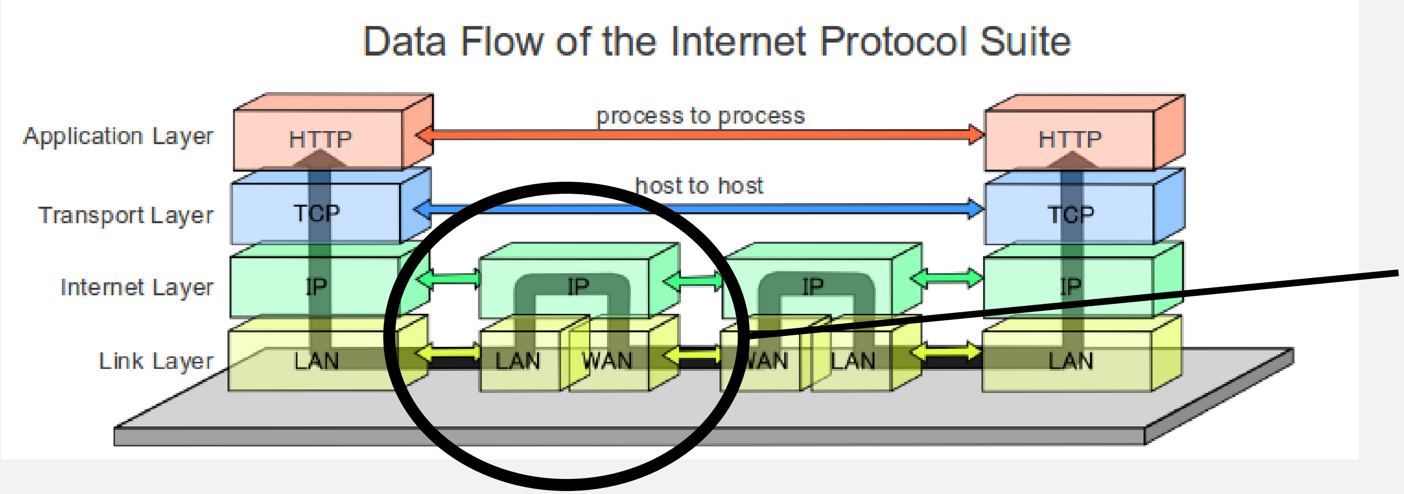
- Firewall developers quickly realized that IP-layer info was insufficient
- Examining TCP packets made it policy enforcement better
  - TCP ports typically represented a specific service
- Policy enforcement mechanism improvements:
  - Policy #1 by blocking access to *ports* not related to required services
  - Policy #3 by blocking outbound requests to unauthorized IP's *or ports*.

LAYER-4 FIREWALL (STATEFUL)

- In addition to examining ports, layer-4 packets also reveal *connection state*
- Some malicious packets violate TCP session rules, for example
- Layer-4 firewalls could also keep track of TCP sessions
- Better enforcement mechanism improvements:
  - Out-of-session packets almost certainly represent a violation of all three policies
  - Servers should not START an out-bound connection

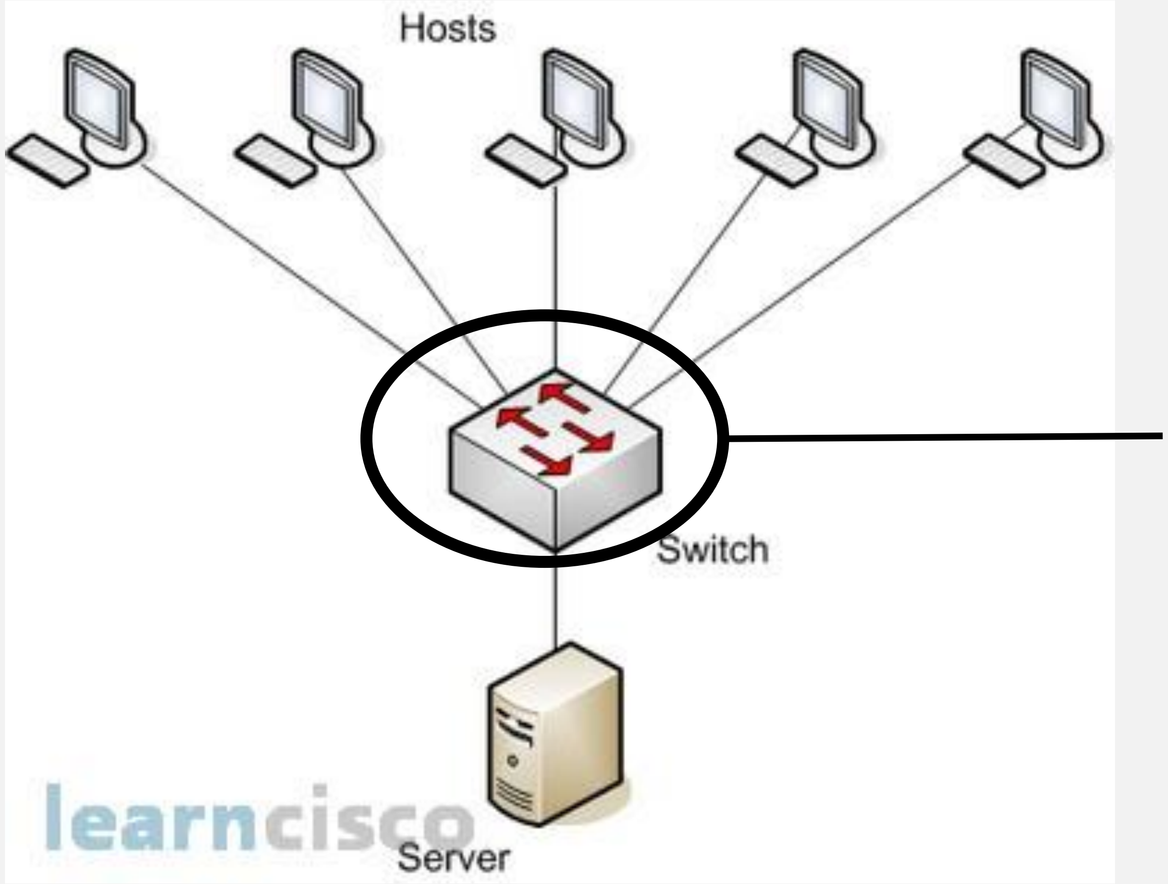
LAYER-4 STILL LAYER-3 ROUTING

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



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

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

- Might be better for enforcing different policies
  - Insider threat policies
  - Different types of devices on the same LAN (e.g., wireless, wired)
- Have some neat defensive properties
  - If only a switch, ***HAS NO IP ADDRESS!!! HARDER TO ATTACK!!!***
  - Called "bump in the wire"

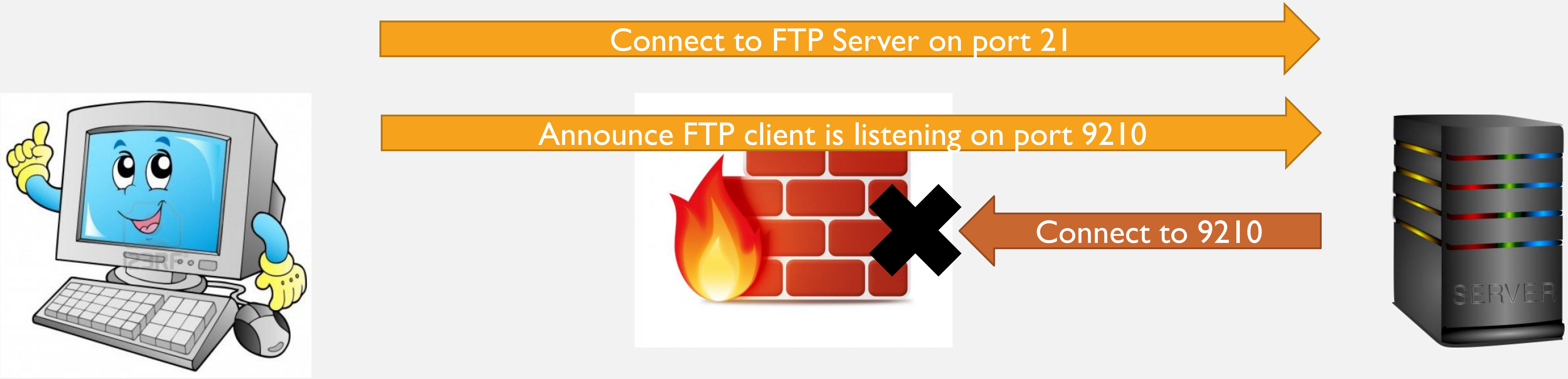
L7 FIREWALLS

- Probably to confuse you personally, L7 refers to the inspection, not the routing
- L7 firewalls examine application data
- Even more "stateful"

EARLY MOTIVATIONS FOR L7

- Application firewalls go back to 1991!!
- The idea was simple: Firewalls should understand application traffic.
- Example: FTP
  - FTP has a control channel and a bulk data channel
  - To transfer a file, a new port is opened dynamically, and communicated over control
  - Even if FTP's control channel port is open, how do you open the dynamic port?

NON FTP AWARE FIREWALL



Connect to FTP Server on port 21

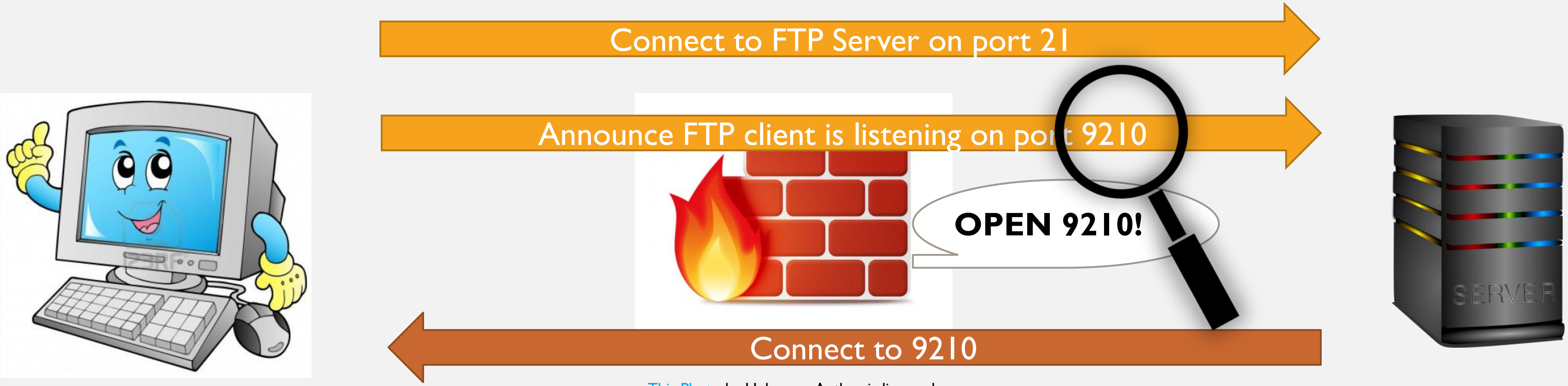
Announce FTP client is listening on port 9210

Connect to 9210

This Photo by Unknown Author is licensed under CC BY-NC

This Photo by Unknown Author is licensed under CC BY-SA

FTP AWARE FIREWALL



Connect to FTP Server on port 21

Announce FTP client is listening on port 9210

OPEN 9210!

Connect to 9210

This Photo by Unknown Author is licensed under CC BY-NC

This Photo by Unknown Author is licensed under CC BY-SA

TRACKING USERS

- Since the early 90's, many firewalls also supported their own services
- Users could connect to the firewall *as a server* and, for example, log-in
- The logging-in process could map a
  - user-name to an IP address
  - Or even a point-to-point protocol with encryption (or VPN)
- Combined with application scanning, far more granular policies enforced

L7+USER POLICY ENFORCEMENT

- Policy #2: Only authorized users from outside the LAN can access LAN resources
- Policy #3: Only authorized users on the LAN can access authorized services outside the LAN

- LAN resources can now be *application specific!*
  - User X can only download on FTP
  - User Y can upload or download on FTP

MORE MOTIVATION FOR L7

- In the past decade, need for L7 scanning has increased
- Consider policy #1 – controlling which services are available
- Without L7, this can only be enforced by monitoring ports.
- What stops a bad person from using an unconventional port number?
- With L7 scanning, can verify the type of traffic

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” (we’ll discuss later)

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 (false positive and false negatives)
- 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 still moving toward 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
- Various products have attempted 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 componets
  - 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 operating systems
  - Purpose: maximum analysis of attacker behavior
- Honeynet – multiple honeypots working together
- Specialized variants:
  - Malware Honeypots
  - Spam Honeypots

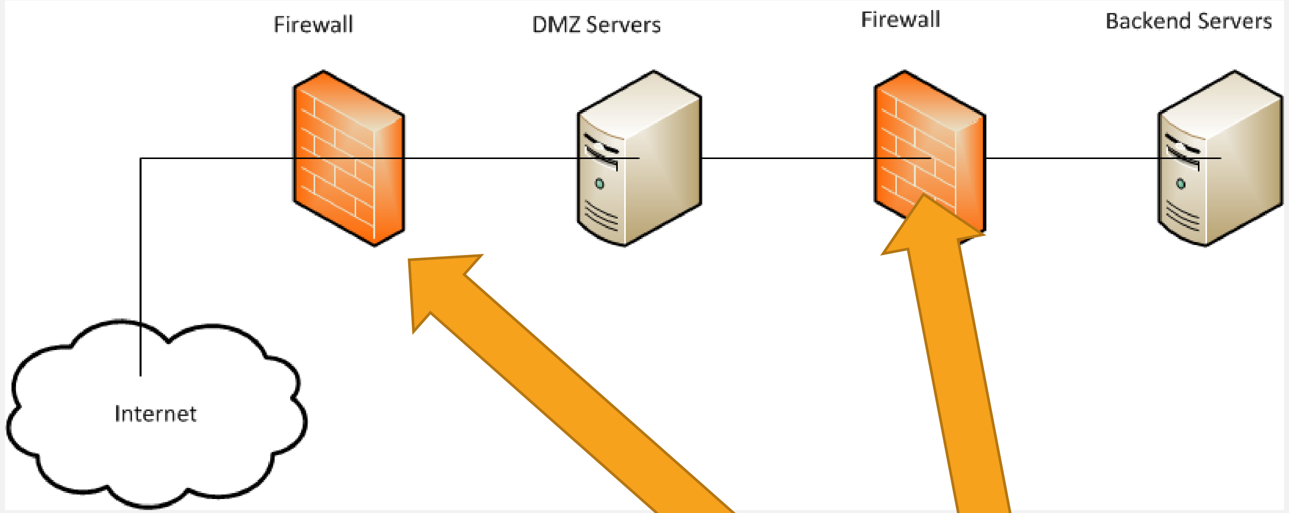
DEPLOYING HONEYPOTS

- Now part of larger "Enterprise Deception Operations" initiatives
- Which type of honeypot makes the most sense?
  - Perhaps counter-intuitively, "low interaction" for corporate
  - "high interaction" for research
  - In the corporate world, may be related to SLA (reaction time, not detail matters)
- But all of this should come back to the security policy, should it not?

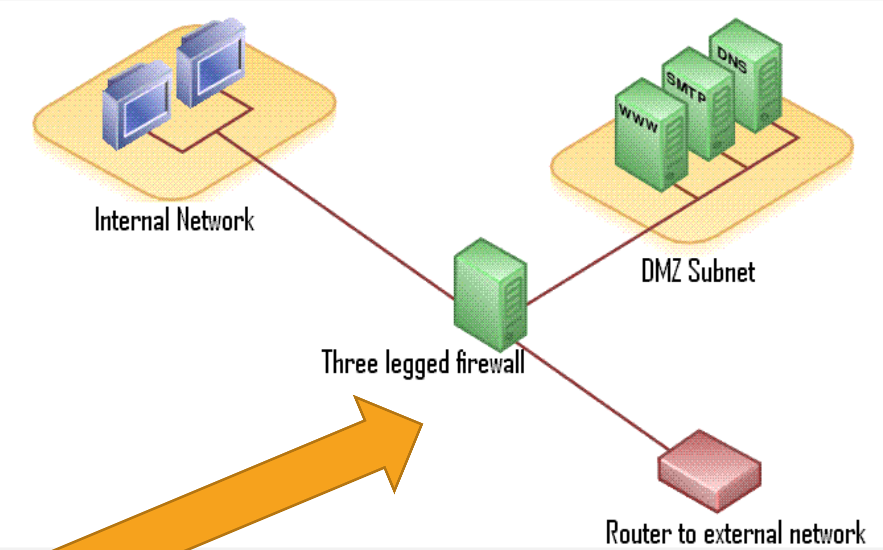
IDS AND SECURITY POLICY

- What policy does IDS (including honeypot) enforce?
- For many (all?) ideal policies, none. The attacker has already violated a policy.
- Perhaps you could think of it as a meta-level policy (policies about policies)
- Or, you could think about it as "enforcement-after-the-fact"
  - That is, how quickly can we get back to compliance?

NETWORK ARCHITECTURE: DMZ



This Photo by Unknown Author is licensed under CC BY-SA



hoto by Unknown Author is licensed under CC BY-SA

POLICY ENFORCEMENT

THE FUTURE

- Later, we'll talk about ***ZERO TRUST NETWORKS***
- Many believe that the "Firewall is Dead", "DMZ's are Dead", etc
- I doubt that they die, but we'll talk later about how they're no longer enough