11/11/26 (make a wish….)





COMP 435: *Computer Security Concepts*

Lecture 31: Network Defenses



The University of North Carolina at Chapel Hill

https://tinyurl.com/comp435-fa26

Plan for Class Today

- 10:10-10:25 – Finish IP/TCP Basics
- 10:25 -11:00 – Network Defenses

If time, start talking about intrusion detection systems, and tunnels (aka VPNS)

Guiding Question ☺

How do we encode rules about what traffic we do/don't want to allow into a network?

Logistics Update

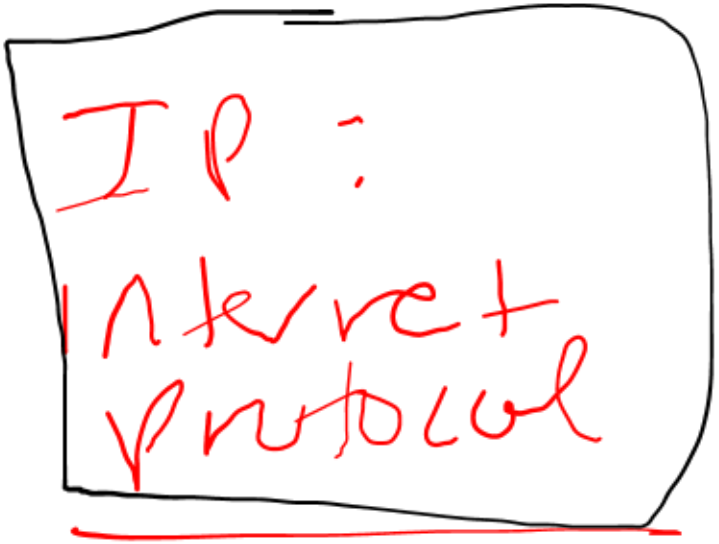


- Written project checkpoint due November 16
  - Worth 15% of the project grade.
- Lab 4 is out. Look at Lec 29.
  - Due 11/18
  - Lab 5 will be in-class!
- WA 5 on Friday!
  - No pre-class component except installing Wireshark!



Some Background: TCP/IP

TCP/IP

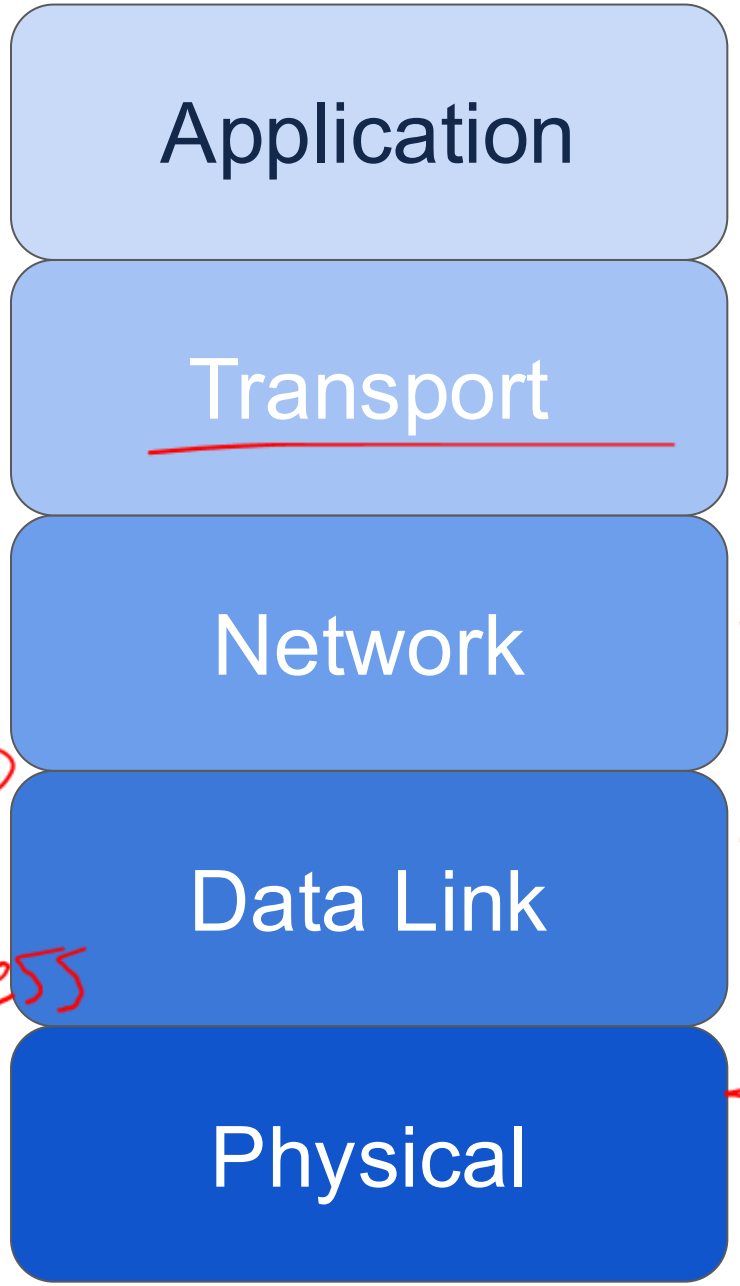




TCP ⟹ Port no.

IP ⟹ address

MAC address



packets

circuit switches

0/1s

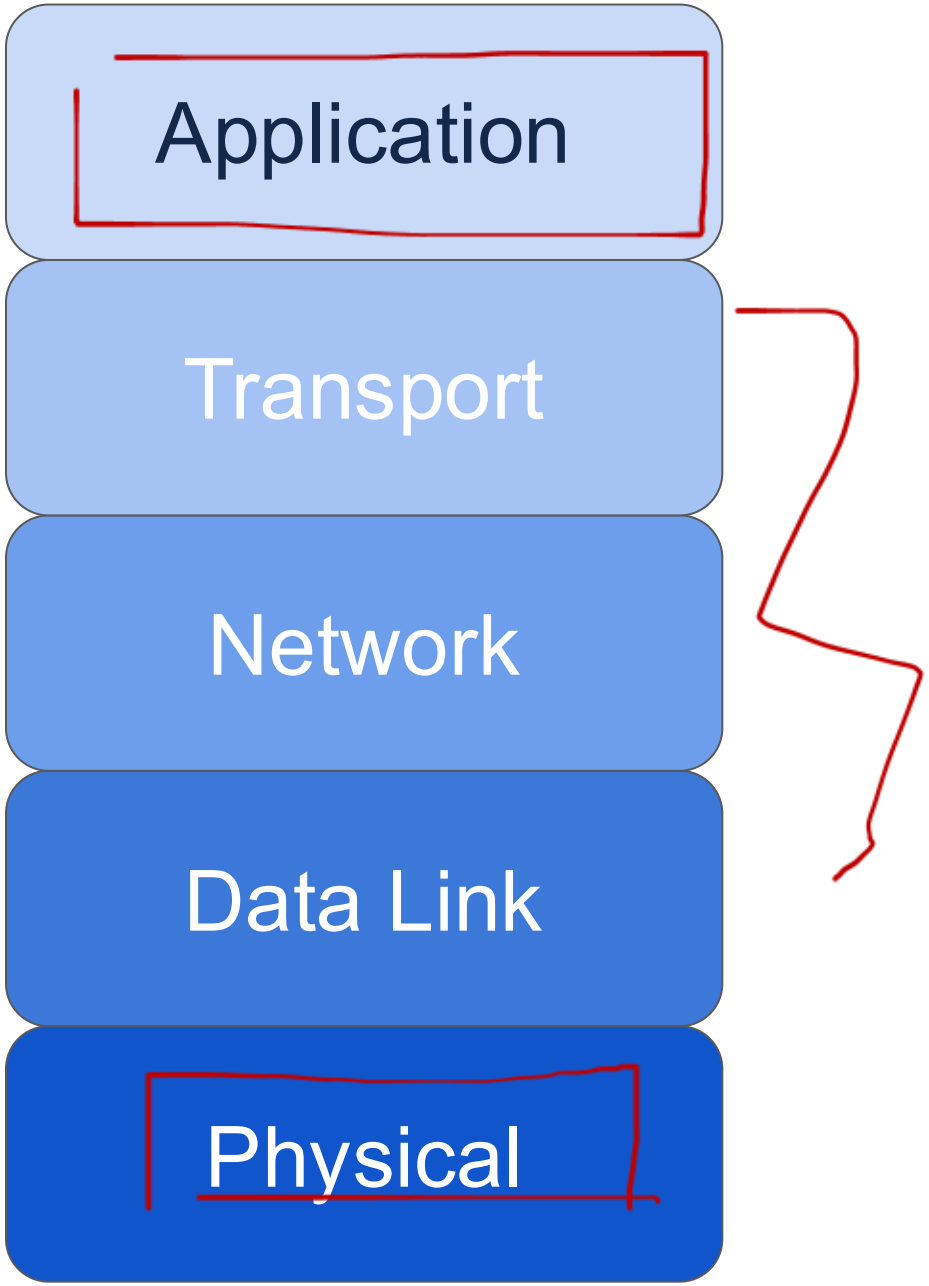
Network Protocol Stack

A layered stack of protocols

Bottom layer: protocols that dictate how bits are transmitted over a wire

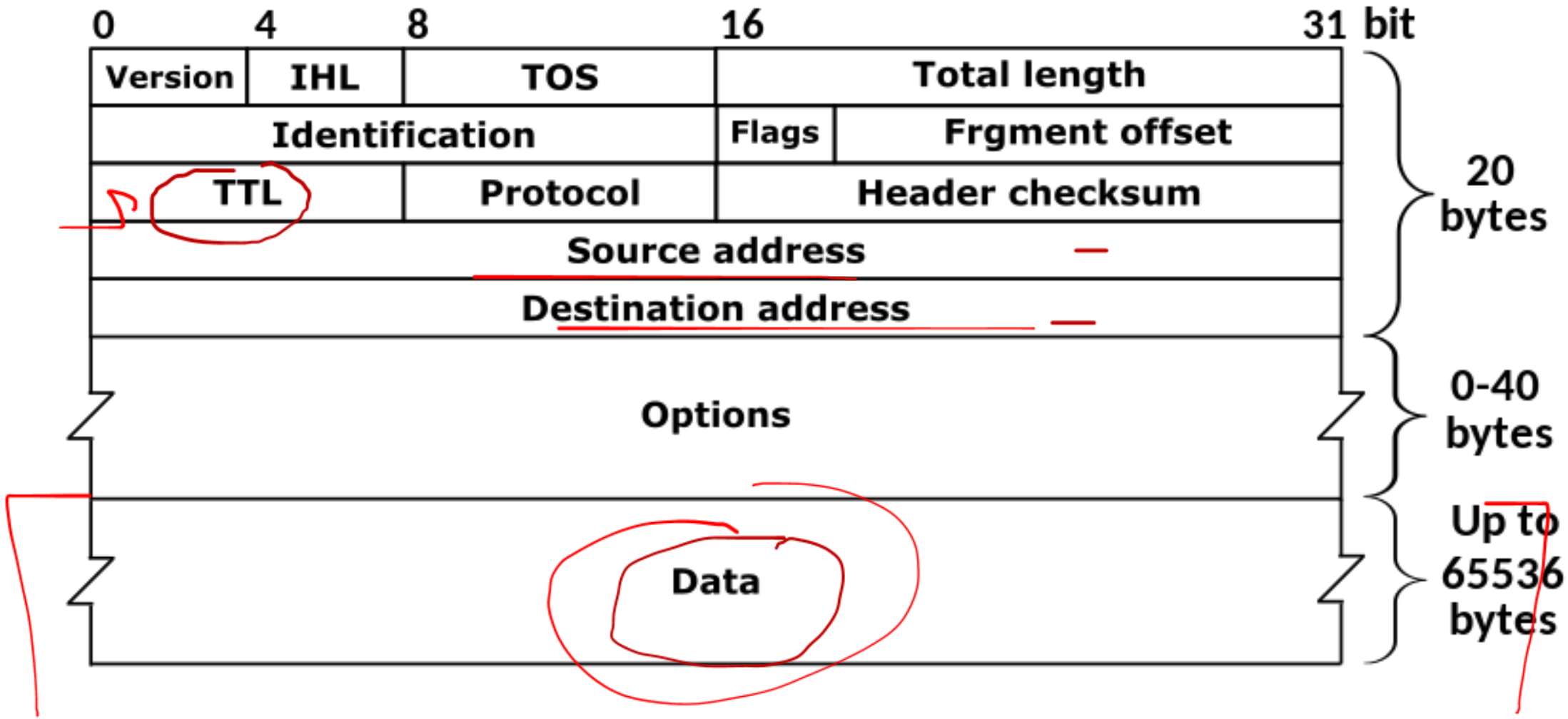
Top layer: protocols that dictate interfaces to applications

Between: local network/internet protocols that dictate how information is routed from one location on internet to another



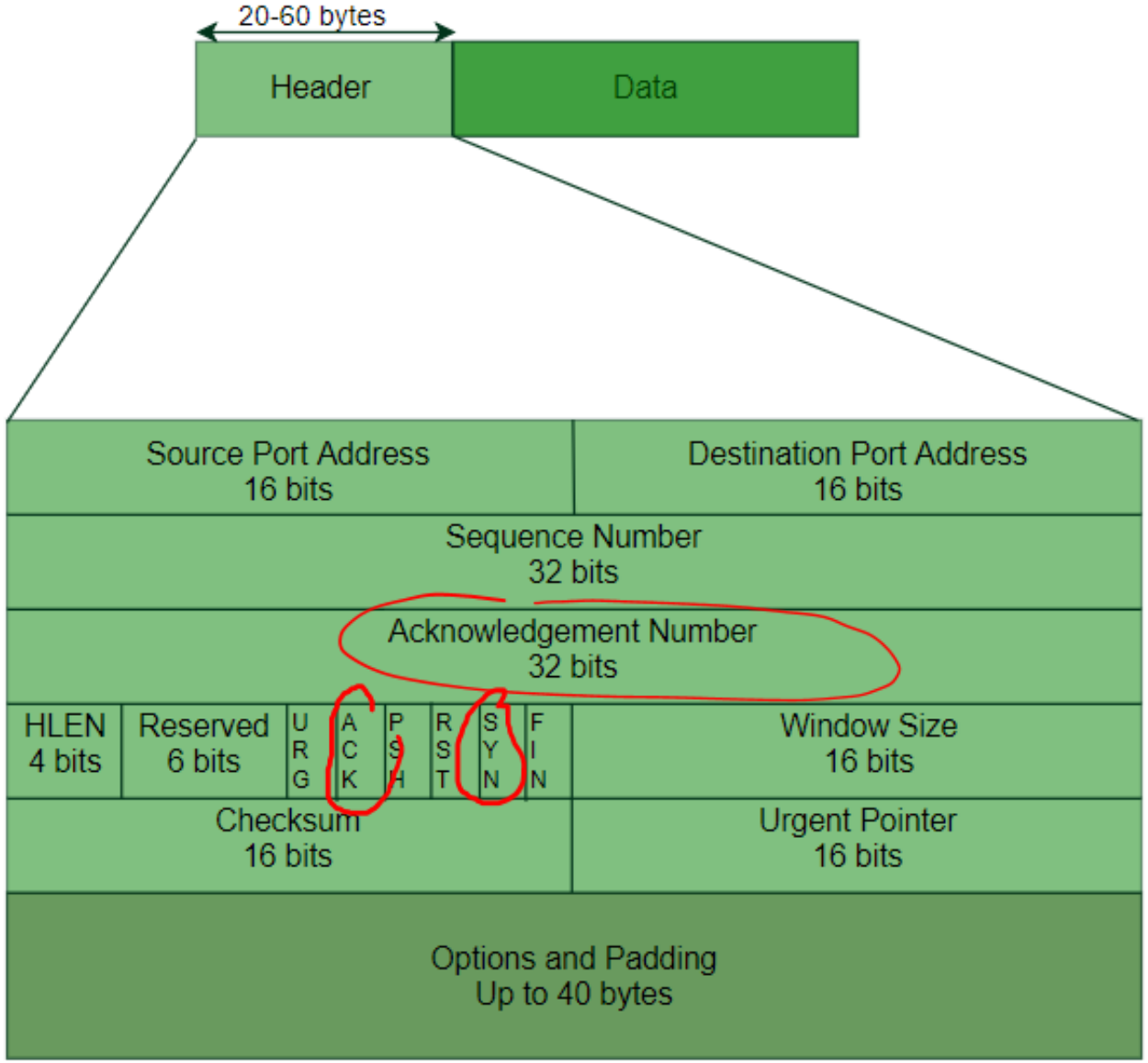
IPv4 Packet

Time-to Live



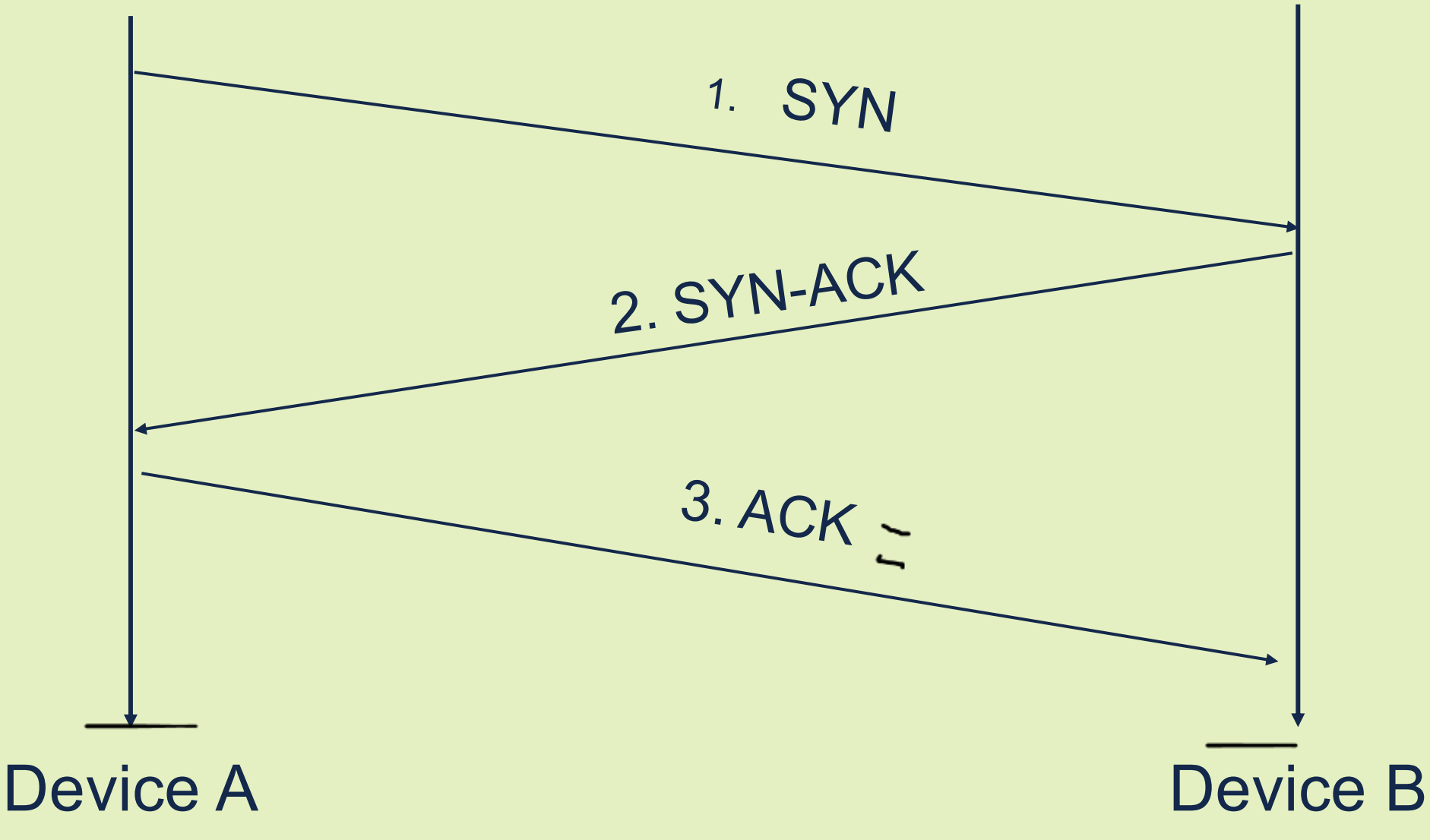
https://en.wikipedia.org/wiki/File:IPv4_Packet-en.svg

TCP Segment



https://www.geeksforgeeks.org/services-and-segment-structure-in-tcp/

TCP





Packet filters

Packet Filter



Def’n: IP packets are compared to a set of rules and either allowed, dropped, or rejected

Filtering Rules

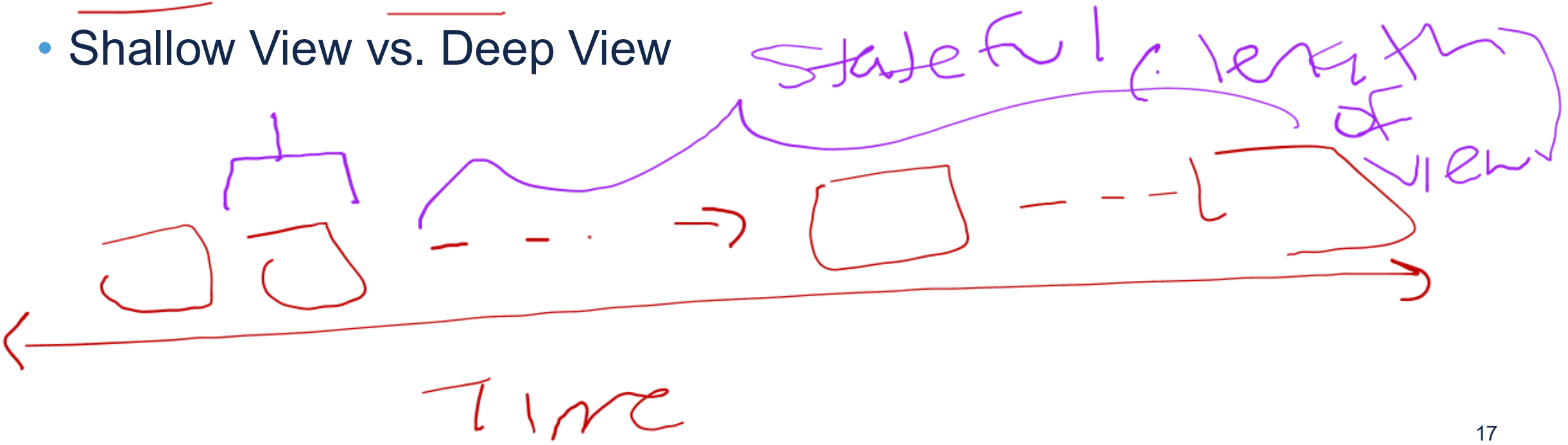


- TCP/IP header fields
- IP header protocol
- Packet size, flags
- Application protocol
- User ID
- Network activity

Ways to Categorize Packet Filters

define good behavior

- Positive vs. Negative — defines bad
  - Ex: Default Deny vs Default Allow
- Stateless vs Stateful
- Shallow View vs. Deep View



Firewall Limitations



- reliance on topology
- untrustworthy insiders
- tunneling
- encrypted content

An Example Packet Filter



Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

An Example Packet Filter

People inside the organization can **receive** mail!

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

An Example Packet Filter

People inside the organization can **send** mail!



Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

– ACK

outbound SMTP connections

Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

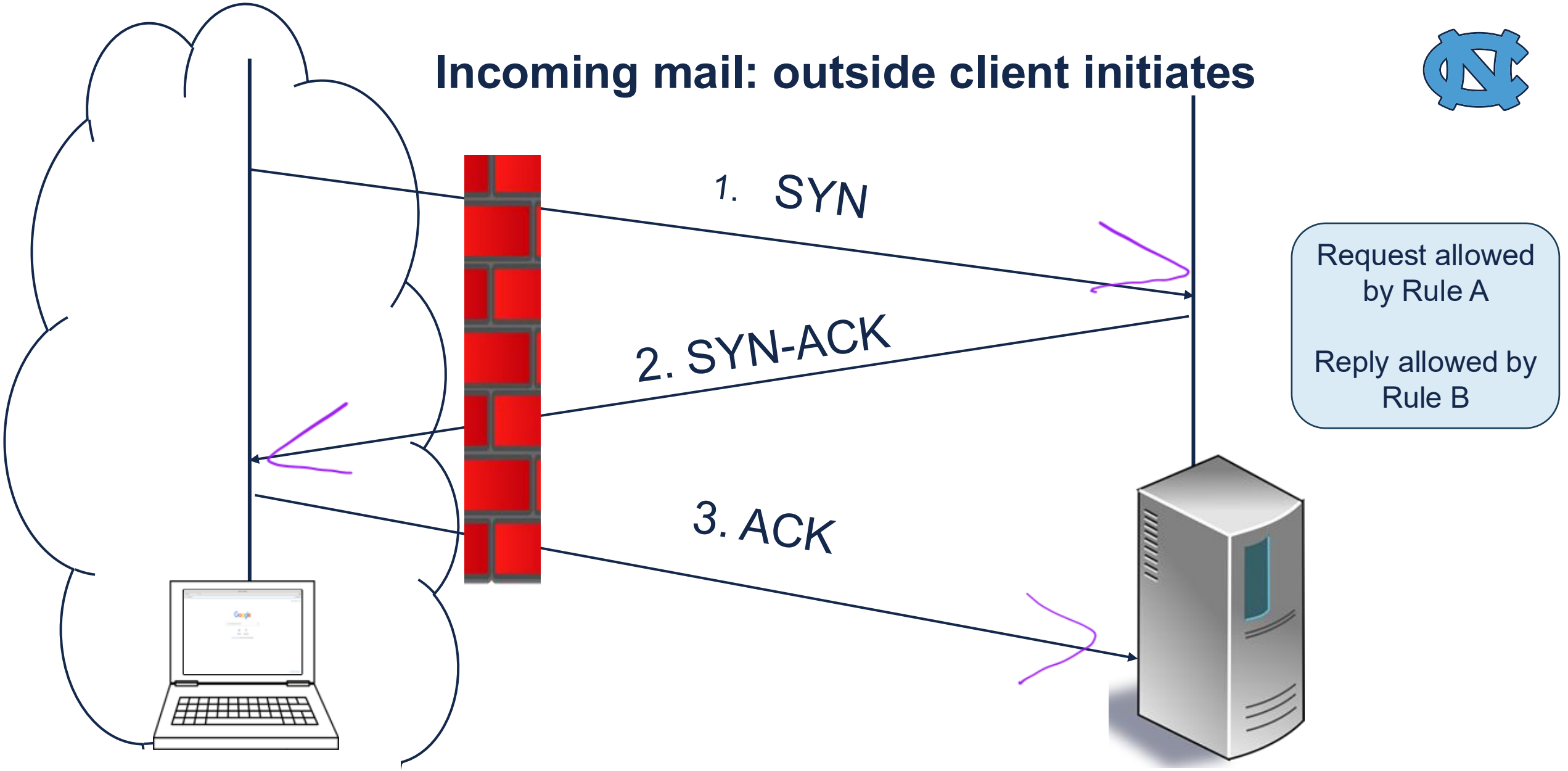
An Example Packet Filter

Default deny!

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

Incoming mail: outside client initiates

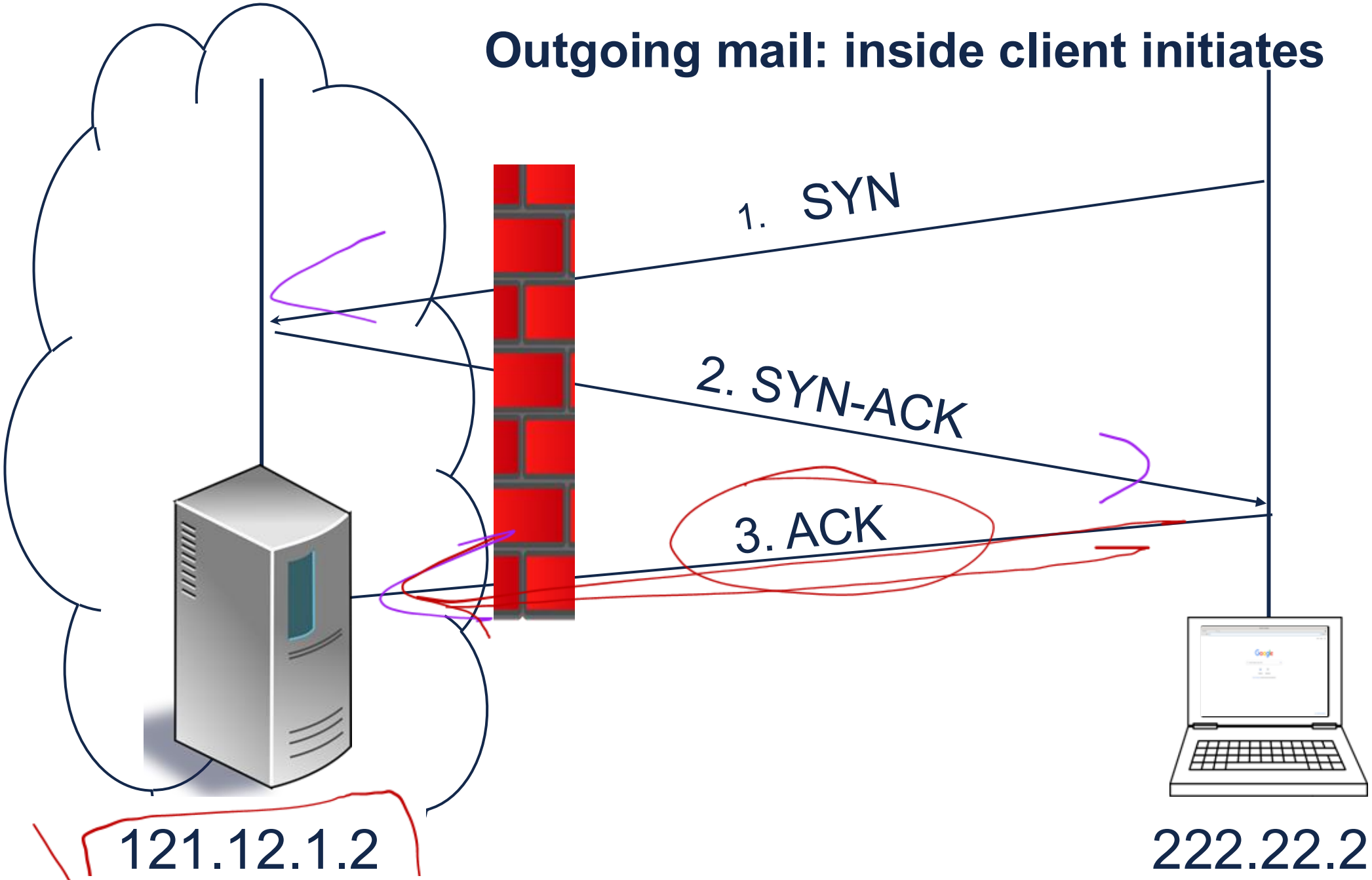


Rule	Dir	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

Packet	Direction	Src	Dest	Protocol	Dest Port	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	25	Allow (A)
2	Out	222.2.2.2	121.12.1.2	TCP	5150	Allow (B)

Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

Outgoing mail: inside client initiates



Request allowed by Rule C

Reply allowed by Rule D

121.12.1.2

External mail server. Port 25

222.22.2.2

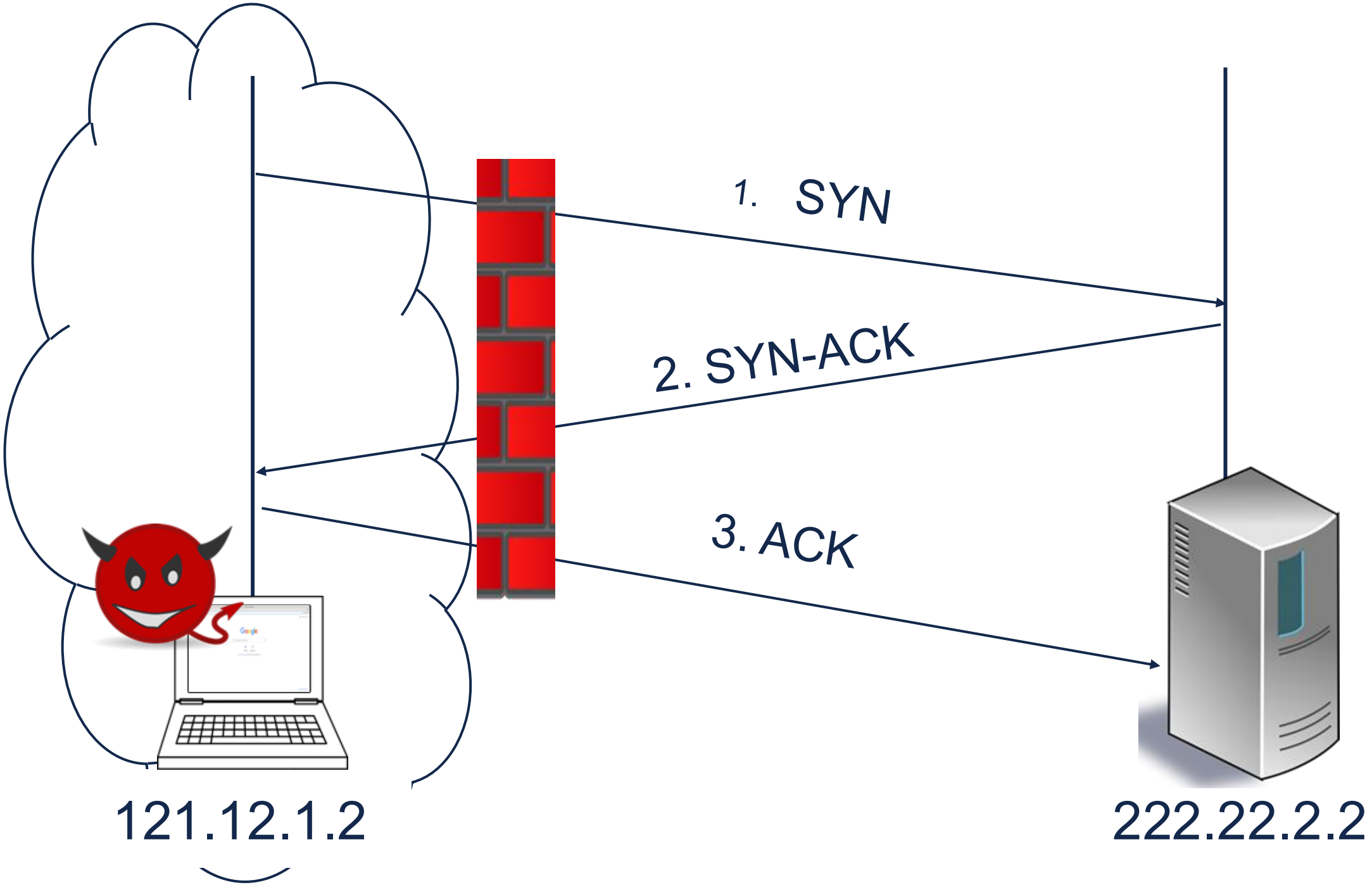
Internal client. Port 5150

An example of what outgoing mail might look like. AKA mail being sent from someone inside org to internet.

Internal mail client uses port 5150

			Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

Packet	Direction	Src	Dest	Protocol	Dest Port	Action (rule)
3	Out	222.22.2.2	121.12.1.2	TCP	25	Permit (C)
4	In	121.12.1.2	222.22.2.2	TCP	5150	Permit (D)


1. SYN
2. SYN-ACK
3. ACK
121.12.1.2
222.22.2.2

A high destination port does not prove a packet is a reply.
Rule D lets an attacker connect to port 8080 from a web proxy server; rule B lets the server reply.

			Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Packet	Direction	Src	Dest	Protocol	Dest Port	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	8080	Allow (D)
2	Out	222.2.2.2	121.12.1.2	TCP	5150	Allow (B)

Updated Packet Filter

One fix: look at source port # as well as destination port #.



Rule	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	Action
A	In	External	Internal	TCP	> 1023	25	Allow
B	Out	Internal	External	TCP	25	> 1023	Allow
C	Out	Internal	External	TCP	> 1023	25	Allow
D	In	External	Internal	TCP	25	> 1023	Allow
E	Either	Any	Any	Any	Any	Any	Deny

Rule	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	Action
A	In	External	Internal				
B	Out	Internal	External	TCP	25	> 1023	Allow
C	Out	Internal	External	TCP	> 1023	25	Allow
D	In	External	Internal	TCP	25	> 1023	Allow
E	Either	Any	Any	Any	Any	Any	Deny

Here are the malicious packets from before. Now, they get denied.



Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	5150	8080	Deny (E)
2	Out	222.2.2.2	121.12.1.2	TCP	8080	5150	Deny (E)

Another attacker: Source port 25 does not prove a packet is a mail server's reply.
An attacker can choose port 25: rule D lets them in, and rule C allows the response.

					Src Port	Dest Port	Action
A	In	External	Internal	TCP	> 1023	25	Allow
B	Out	Internal	External	TCP	25	> 1023	Allow
C	Out	Internal	External	TCP	> 1023	25	Allow
D	In	External	Internal	TCP	25	> 1023	Allow
E	Either	Any	Any	Any	Any	Any	Deny

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	25	8080	Allow (D)
2	Out	222.2.2.2	121.12.1.2	TCP	8080	25	Allow (C)

Fix: including the ACK flag in the rules

			Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action
A	In	External	Internal	TCP	> 1023	25	Any	Allow
B	Out	Internal	External	TCP	25	> 1023	Yes	Allow
C	Out	Internal	External	TCP	> 1023	25	Any	Allow
D	In	External	Internal	TCP	25	> 1023	Yes	Allow
E	Either	Any	Any	Any	Any	Any	Any	Deny

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	25	8080	No	Deny (E)

Rule	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action
A	In	External	Internal	TCP	> 1023	25	Any	Allow
B	Out	Internal	External	TCP	25	> 1023	Yes	Allow
C	Out	Internal	External	TCP	> 1023	25	Any	Allow
D	In	External	Internal	TCP	25	> 1023	Yes	Allow
E	Either	Any	Any	Any	Any	Any	Any	Deny

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
1	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	25	8080	Yes	?? (?)

Rule	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action
A	In	External	Internal	TCP	> 1023	25	Any	Allow
B	Out	Internal	External	TCP	25	> 1023	Yes	Allow
C	Out	Internal	External	TCP	> 1023	25	Any	Allow
D	In	External	Internal	TCP	25	> 1023	Yes	Allow
E	Either	Any	Any	Any	Any	Any	Any	Deny

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
1	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	5051	25	Yes	?? (?)



Rule	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action
A	In	External	Internal	TCP	> 1023	25	Any	Allow
B	Out	Internal	External	TCP	25	> 1023	Yes	Allow
C	Out	Internal	External	TCP	> 1023	25	Any	Allow
D	In	External	Internal	TCP	25	> 1023	Yes	Allow
E	Either	Any	Any	Any	Any	Any	Any	Deny

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
1	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	25	5055	Yes	?? (?)



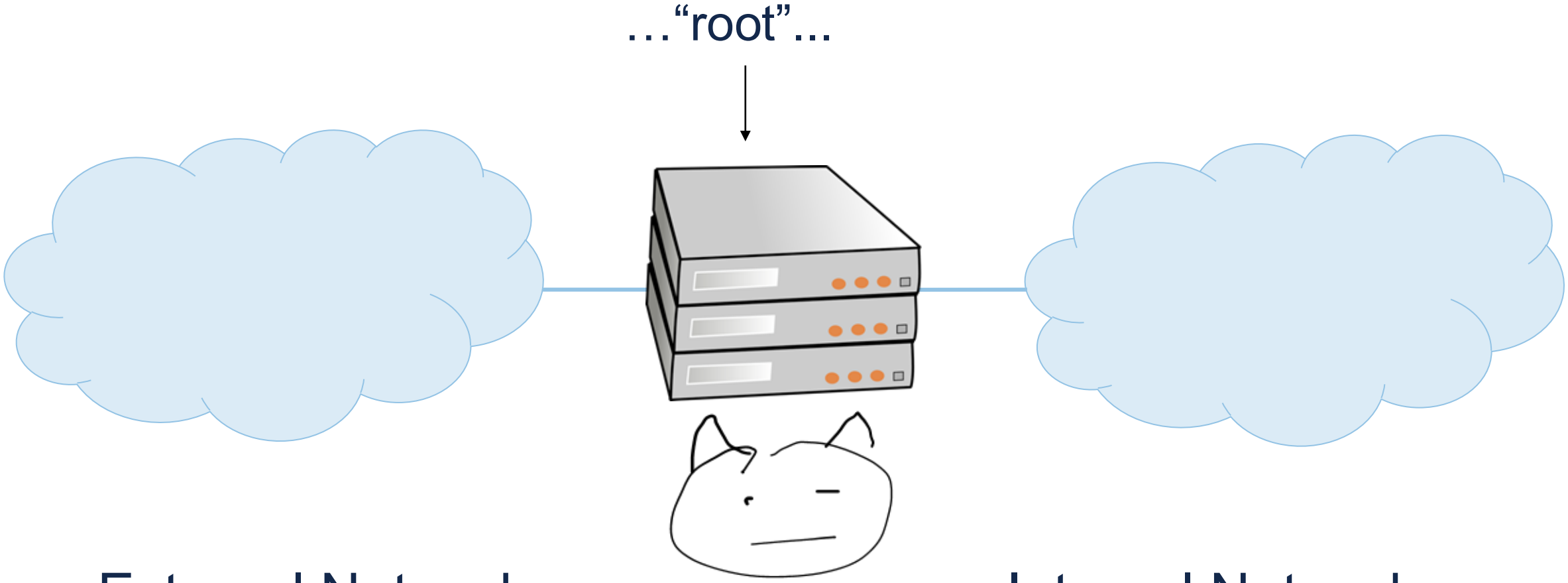
Problem: packet filters have an imperfect view

Signature-Based Filters



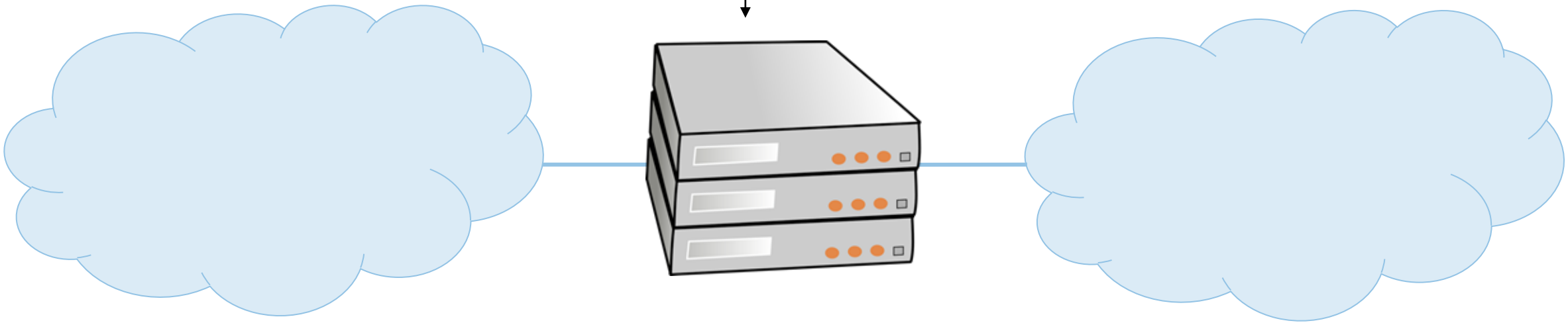
Def'n: a packet filter that inspects the packet payload to find patterns of known attacks

E.g., look for "root"; look for "/etc/passwd"


…“root”...
External Network
Internal Network

grep

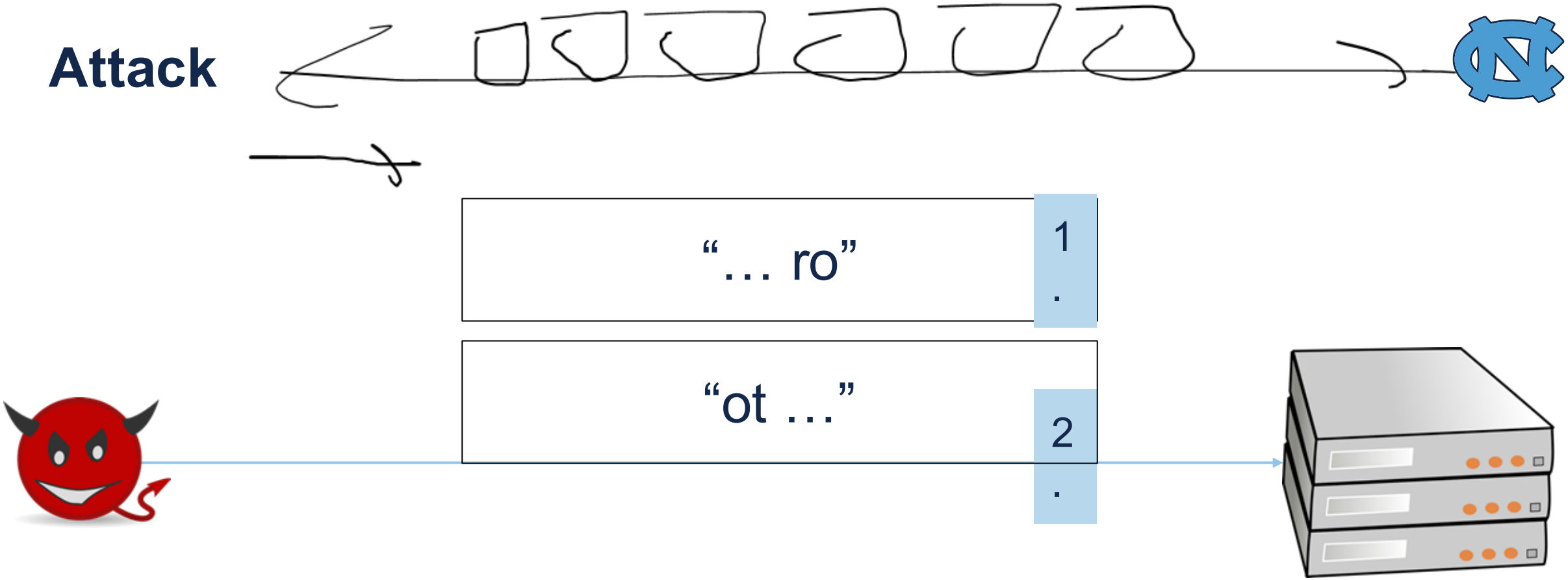
IP Header | TCP Header | “....root…”



External Network

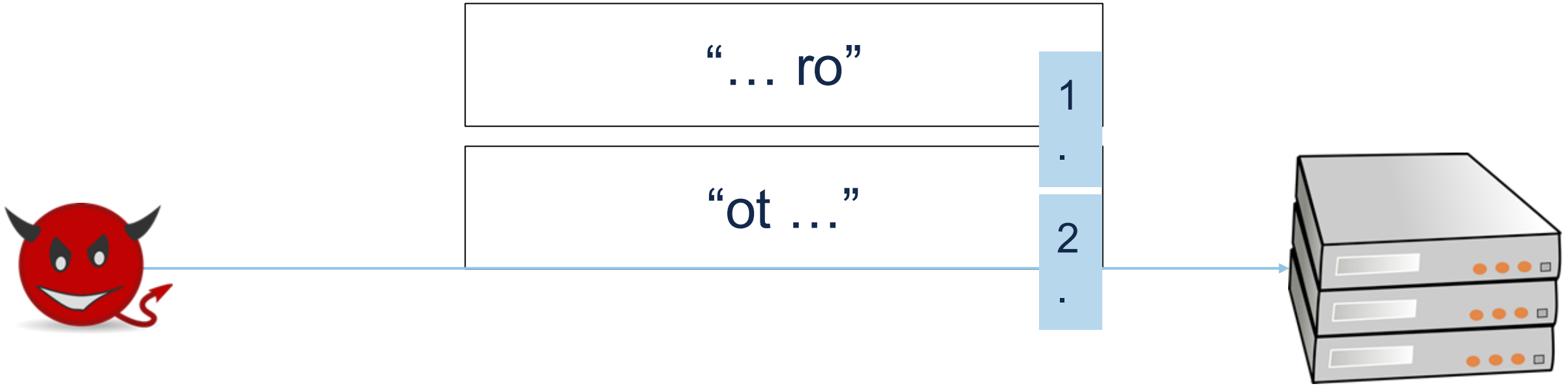
Internal Network

Attack



Neither segment contains “root,” but the reassembled stream does. Inspecting packets individually can miss content split across boundaries.

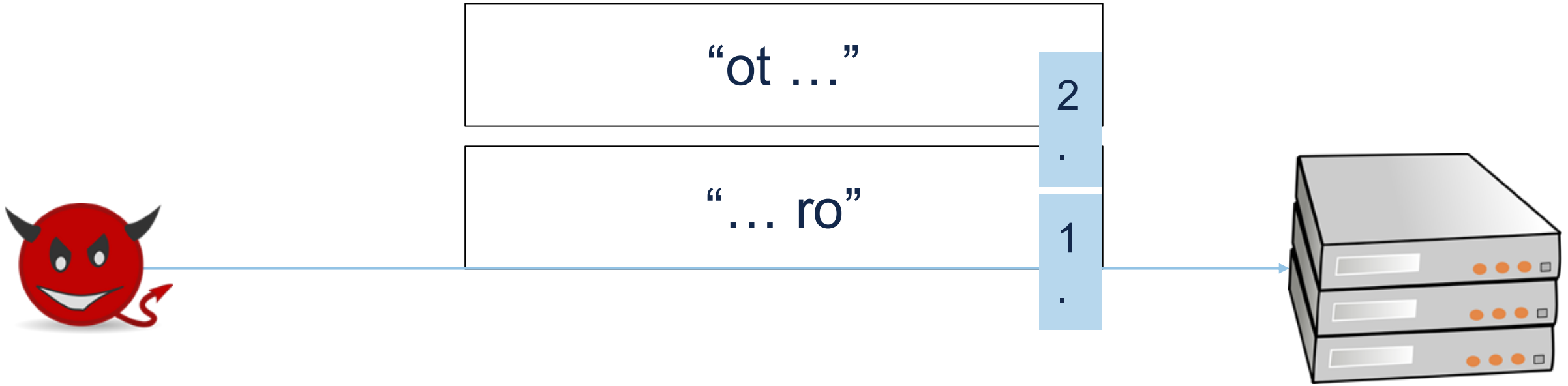
Attack



Fix: Track sequences of packets

Downside…. Have to track more state.

Attack



Attacker can easily ensure segments sent out of order.

Another Attack

TTL=25	“r”
TTL=19	“i”
TTL=25	“o”
TTL=19	“p”
TTL=25	“o”
TTL=25	“t”



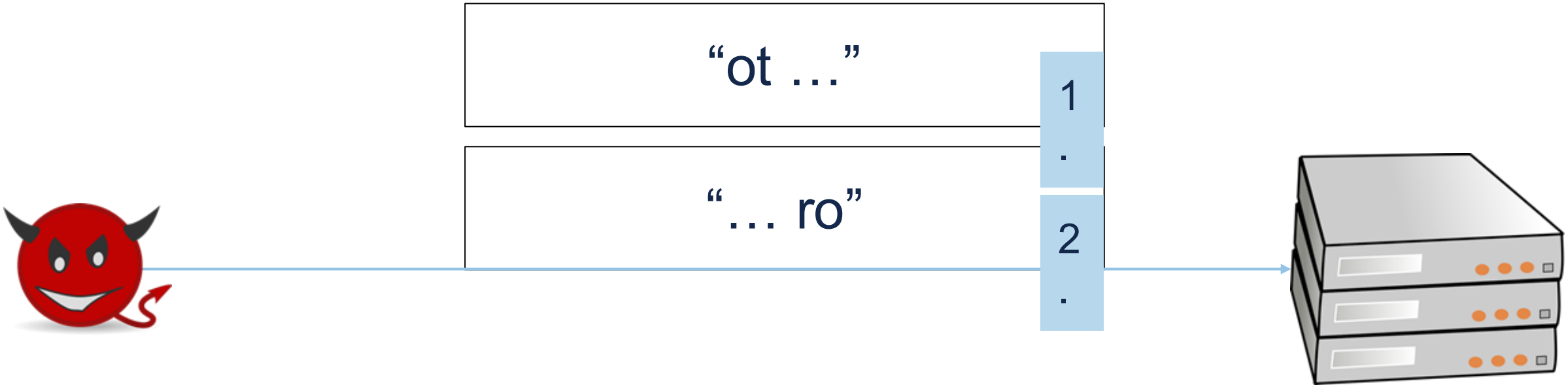


r

o

o

t



Fix: Reassemble the TCP stream



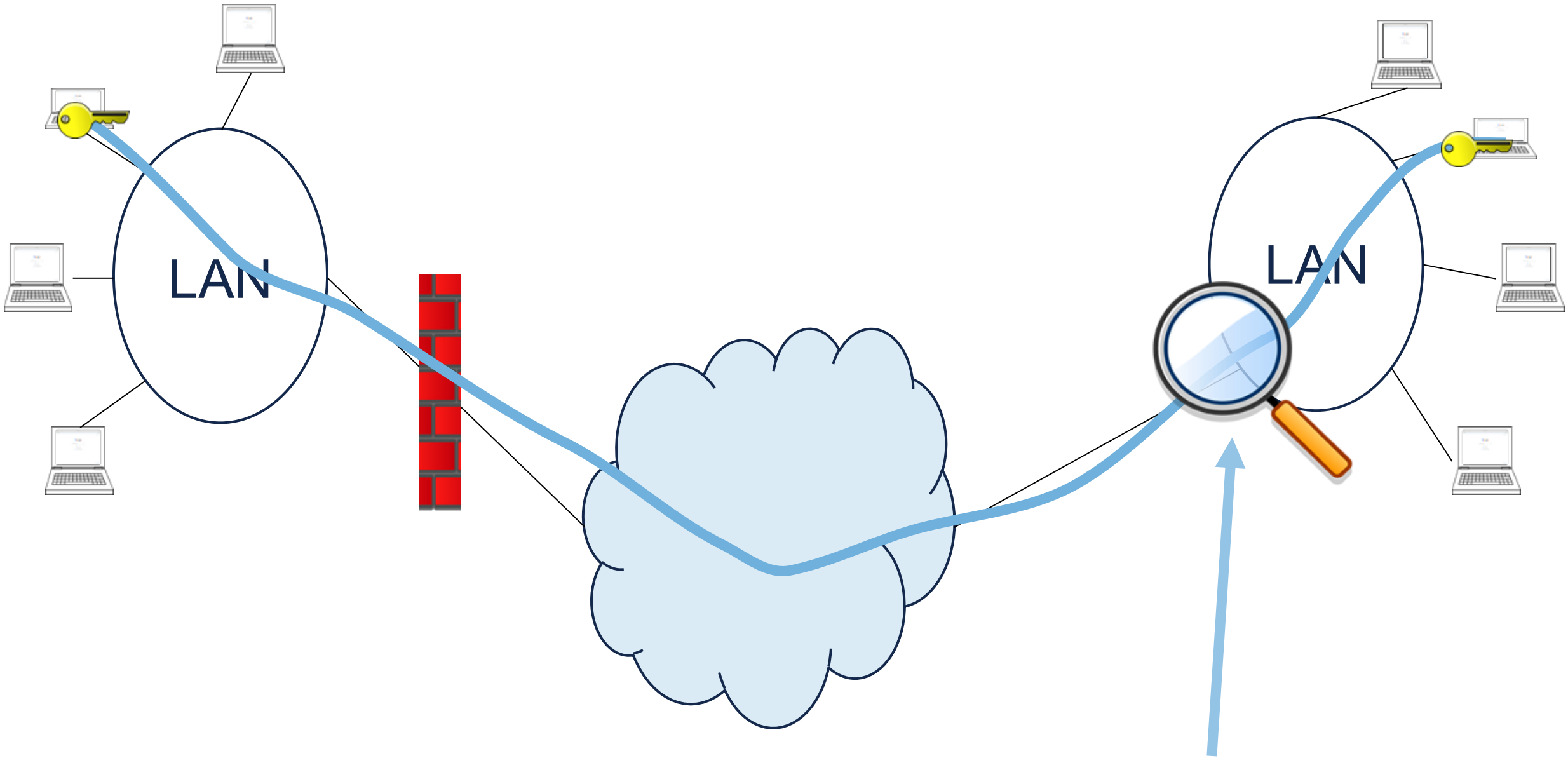
a) Dolev-Yao
↳ good/valid user can't
- make us/be user
- employee leaves w/ infected laptop w/ USB
- phishing

Q2 from Lecture 30 Practice

b)
firewall can't fully protect
in the ex: split, encrypted



Intrusion Detection Systems


LAN
LAN

Intrusion

Def'n: an event on a host or network that violates the desired security policy

A.k.a. incident

E.g., unauthorized connection, illegal program execution

Intrusion Detection System (IDS)



Def’n: automated process that monitors events and alerts a human to potential harm

Intrusion Detection Systems (IDS)

- Supports forensic analysis
- Monitors and logs events
- Alerts human to adverse events

Intrusion Prevention Systems (IPS)

- Responds to events
- Block or alter events
- Alerts human to adverse events

Network-Based Intrusion Detection Systems (NIDS)

- Network-wide viewpoint
- Doesn't touch endpoints
- Events: packets

Host-Based Intrusion Detection Systems (HIDS)

- Single host viewpoint
- Not blocked by encryption
- Events:
  - log updates
  - filesystem changes
  - system calls
  - CPU use