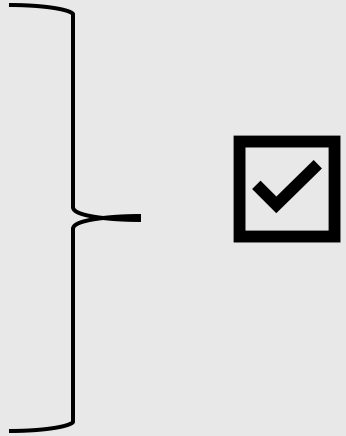
COMP435: *SECURITY CONCEPTS!*

Lecture 17: Intro to Network Security

tinyurl.com/comp435-fa25

Course Outline: ~6 Units

- Introduction to Security Concepts + Principles
- Cryptography
- Systems/OS Security
- Software Security
- Network Security
- Web Security
- *Bonus* Misc Unit at the End ☺



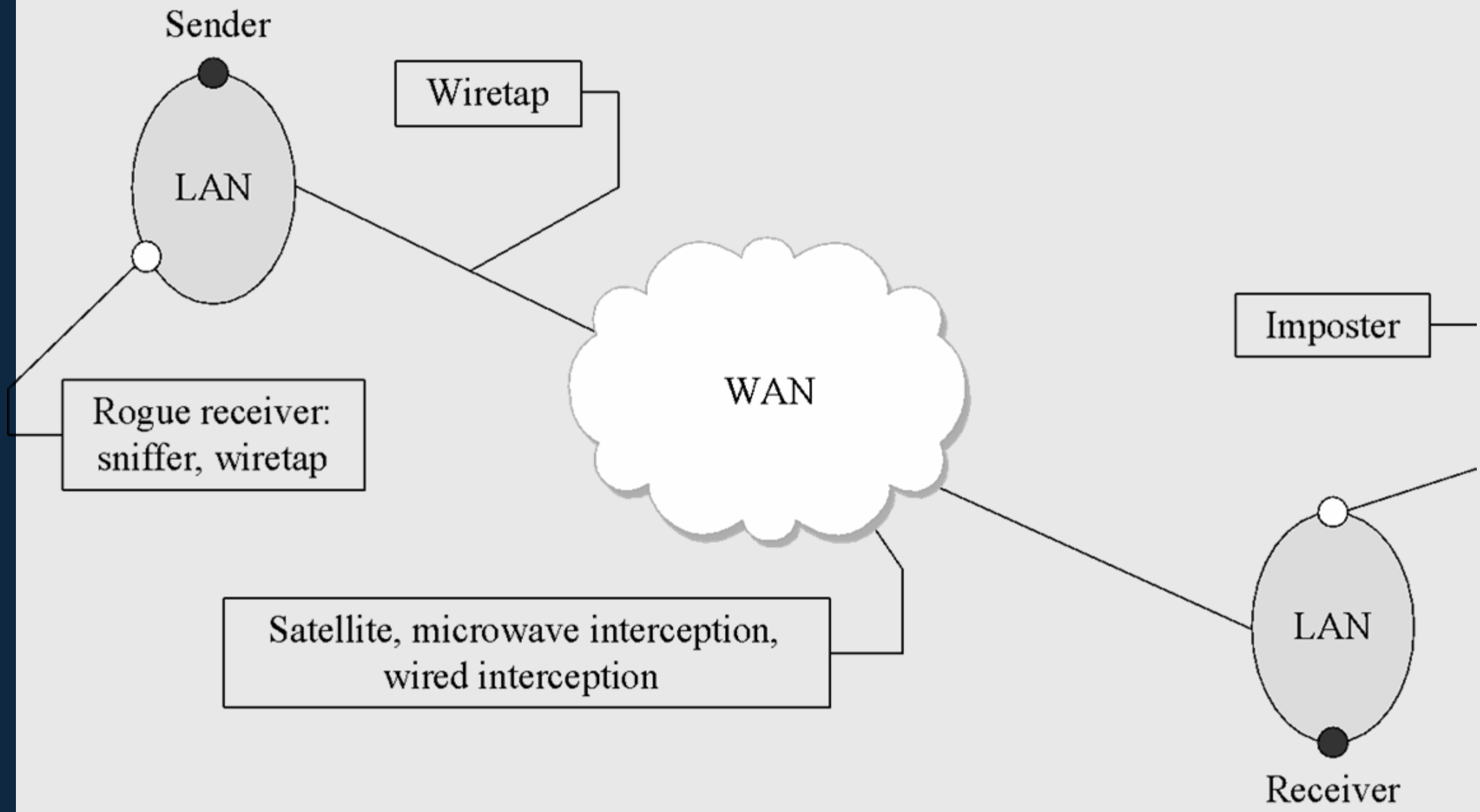
Quiz Topics & Logistics Updates

- Access Control Mechanisms
  - *Discretionary Access Control & Access Control Matrices*
  - *Bell LaPudula Model & Biba Integrity Model*
- Software Vulnerabilities – Should be familiar with the ones we studied in class and in the lab(s). How to identify the presence of a bug and potentially fix it if given a code listing.
  - *Heartbleed*
  - *Buffer overflow/overrun*
  - *Integer overflow/overrun*
  - *Confused deputy*
- New lab & WA out now!

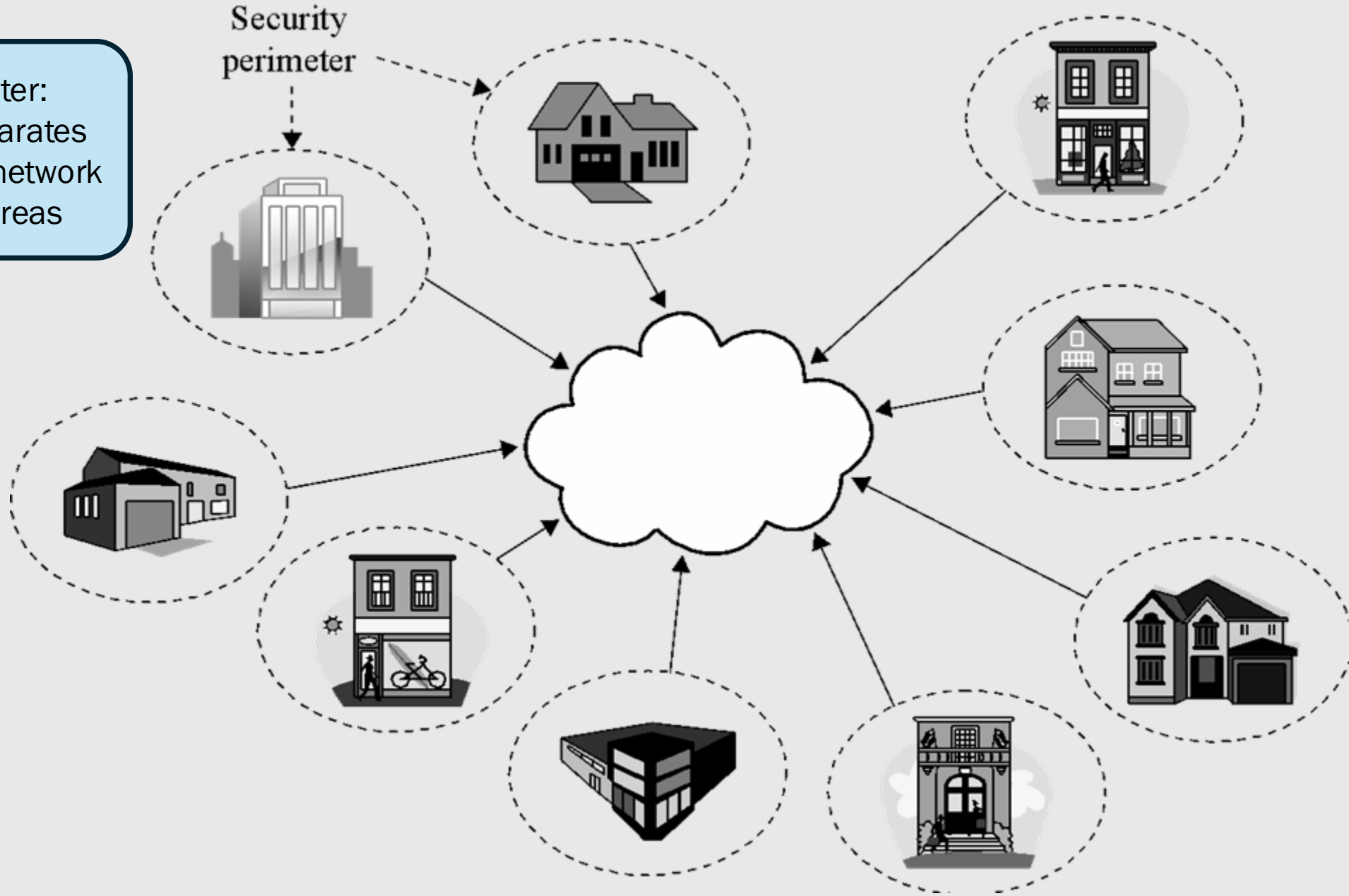
NETWORK SECURITY CONCEPTS

Challenges

- Anonymity
- Many points of attack
- Sharing
- Complexity
- Unknown perimeter
- Unknown path



Security perimeter: boundary that separates trusted part of the network from untrusted areas



Medium	Strengths	Weaknesses
Wire	• Cheap • Ubiquitous	• Signal emanation • Physical wiretapping
Optical Fiber	• No emanation • No wiretapping	• Weak at connection points
Microwave	• Strong signal	• Interception possible • Line of sight needed • Needs repeaters
Wireless	• Ubiquitous	• Interception possible • Short range
Satellite	• Strong signal	• Delay (long distance) • Interception possible

Threats

- Interception
- Modification
- Fabrication
- Interruption

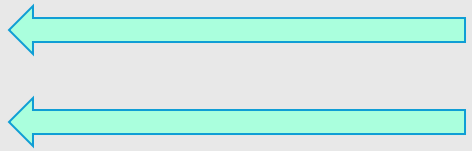
Threats

- Interception
- Modification
- Fabrication
- Interruption

confidentiality

Threats

- Interception
- Modification
- Fabrication
- Interruption



integrity

Threats

- Interception
- Modification
- Fabrication
- Interruption

availability

DOLEV-YAO MODEL

Dolev-Yao Model

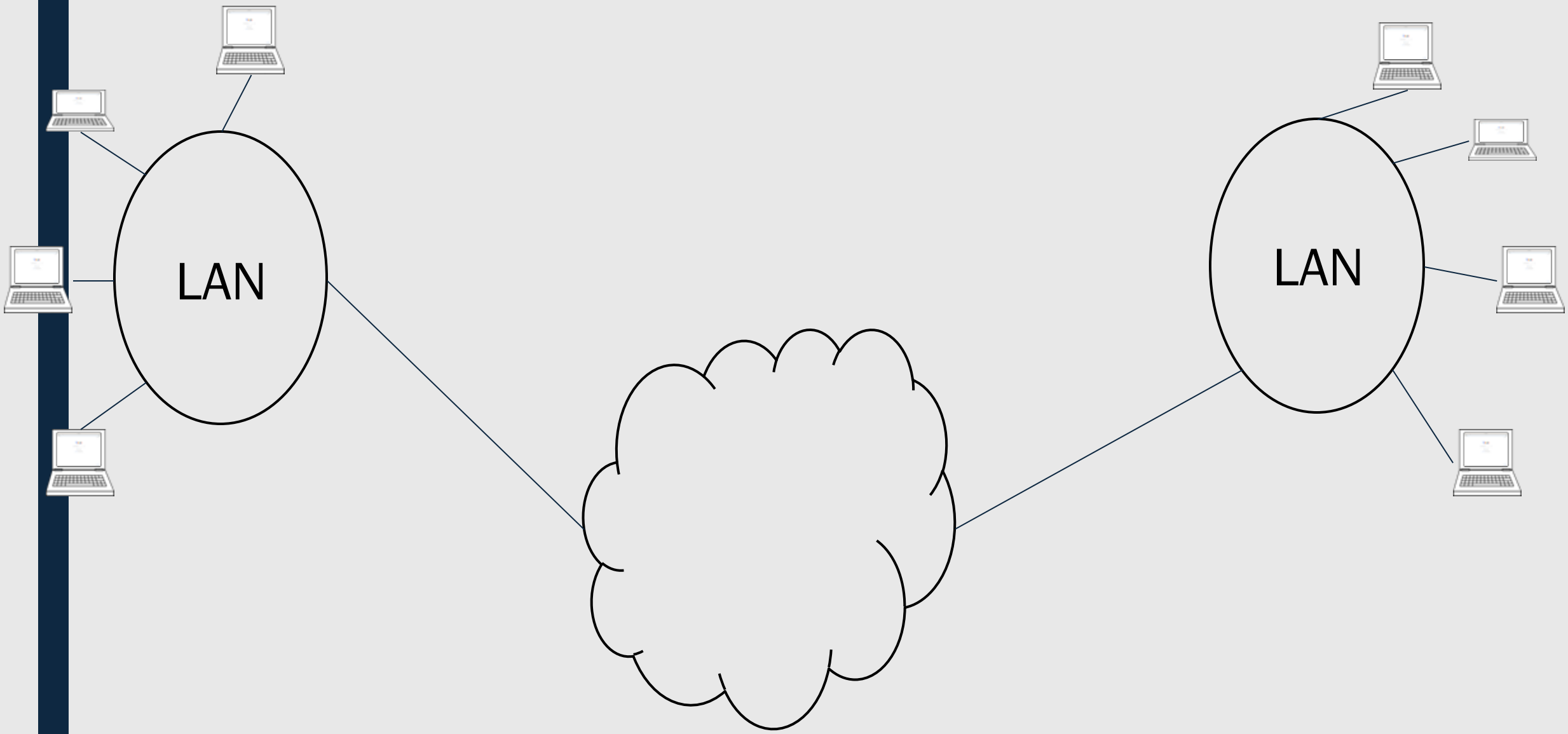
- IEEE Transactions on Information Theory, 1983
- Active attacker
  - *Is a legitimate user of the network*
  - *Can obtain any message on the network*
  - *Can be a receiver to any user*

Dolev-Yao Model

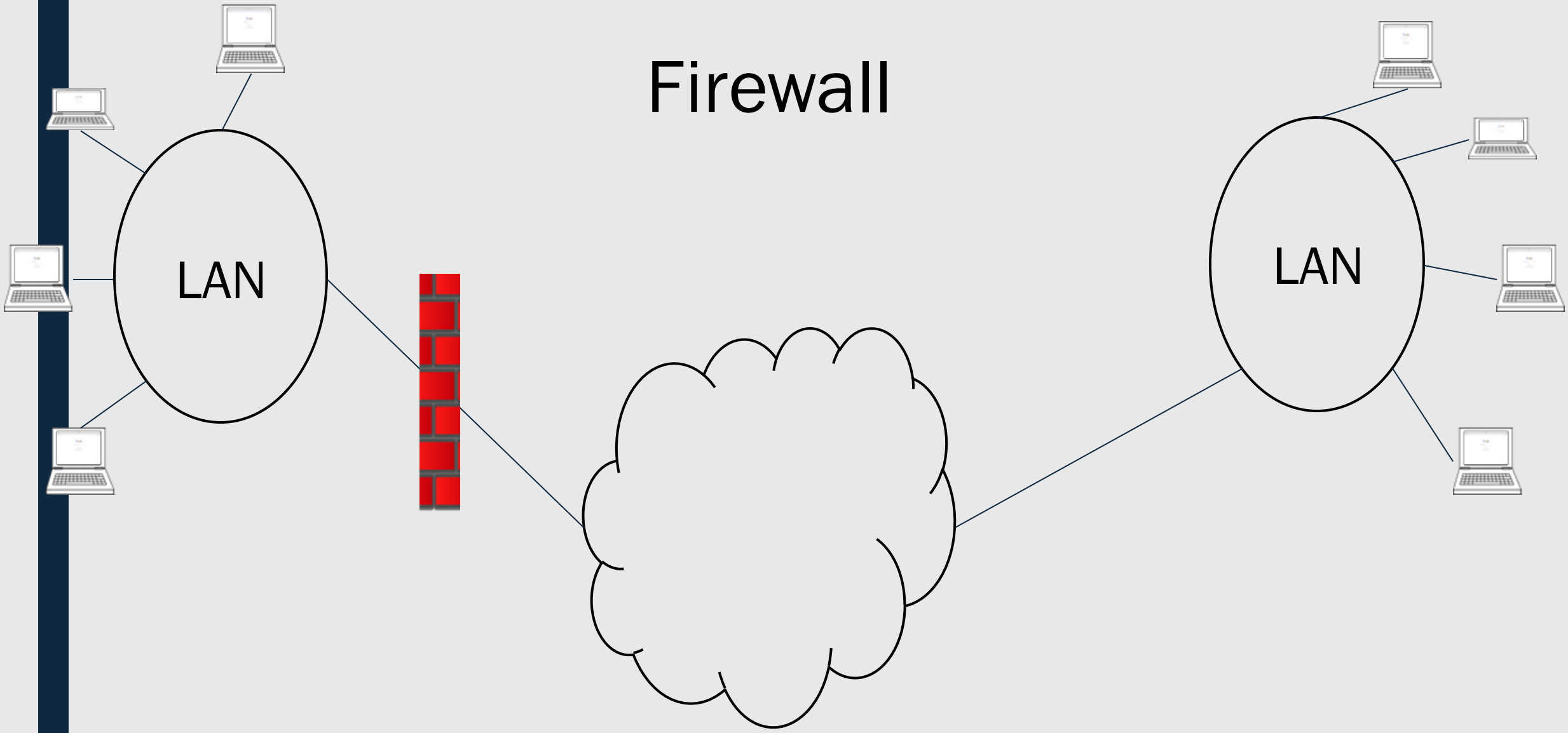
- IEEE Transactions on Information Theory, 1983
- Active attacker
  - *Is a legitimate user of the network*
  - *Can obtain any message on the network*
  - *Can be a receiver to any user*

The attacker carries the message

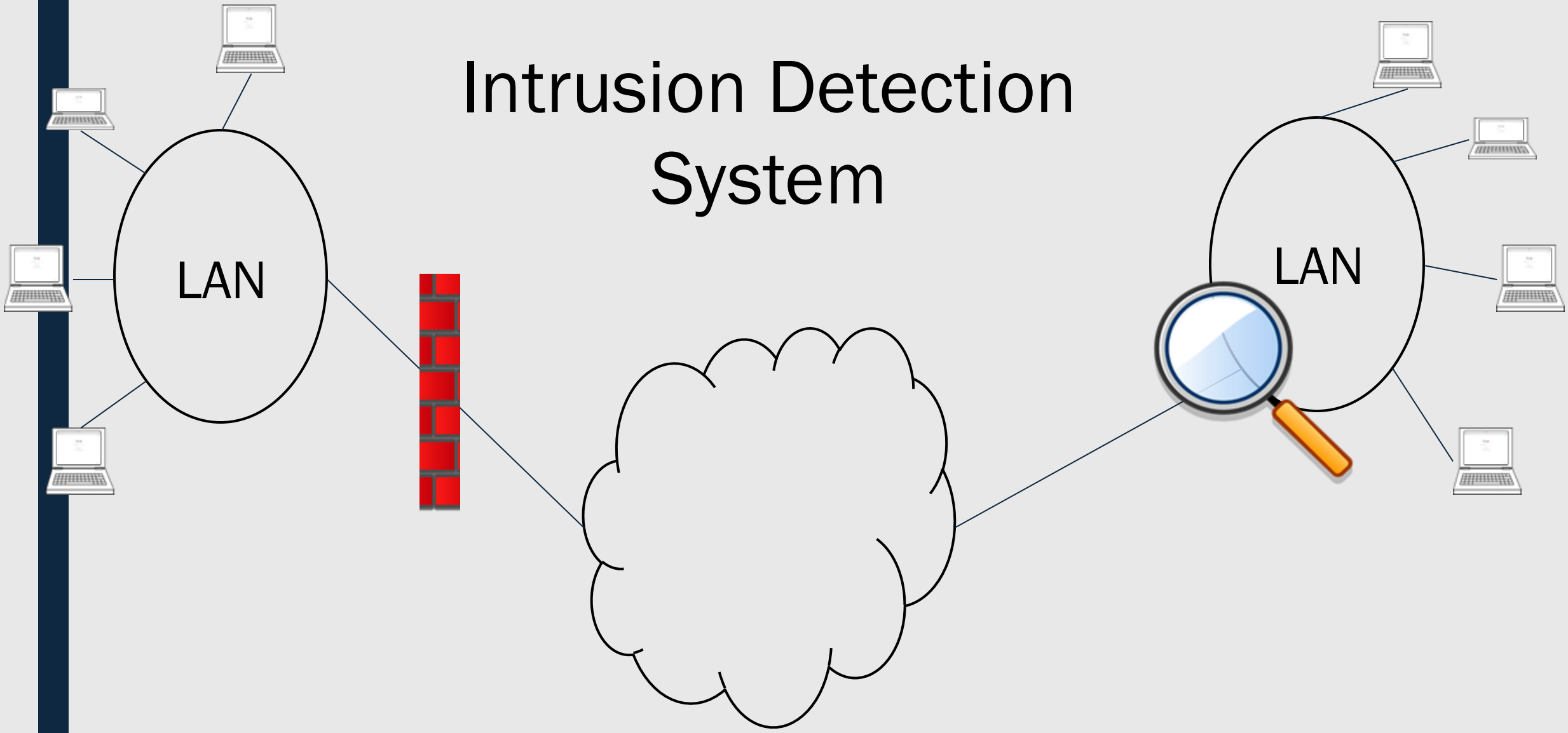
DEFENSE STRATEGIES


LAN
LAN

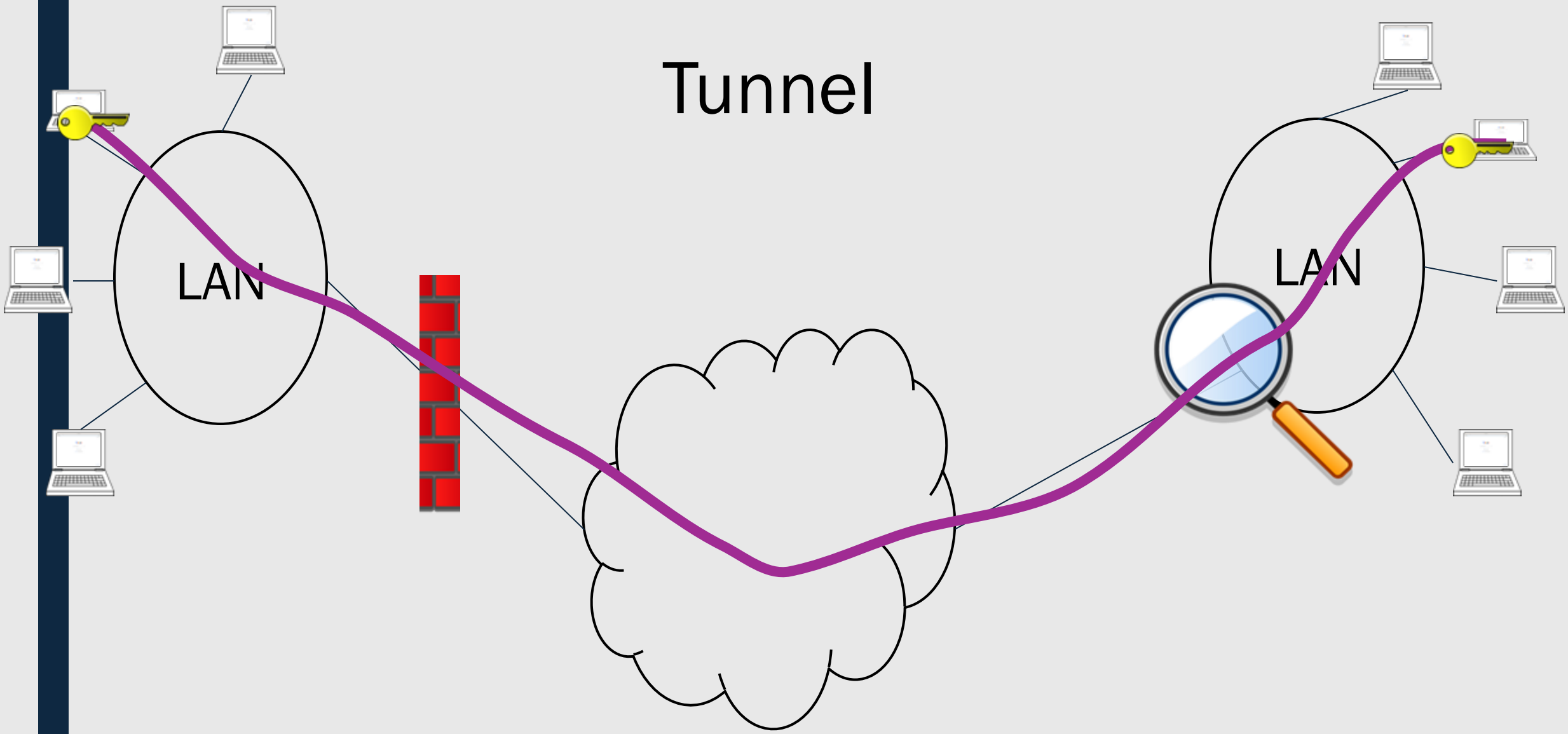
Firewall



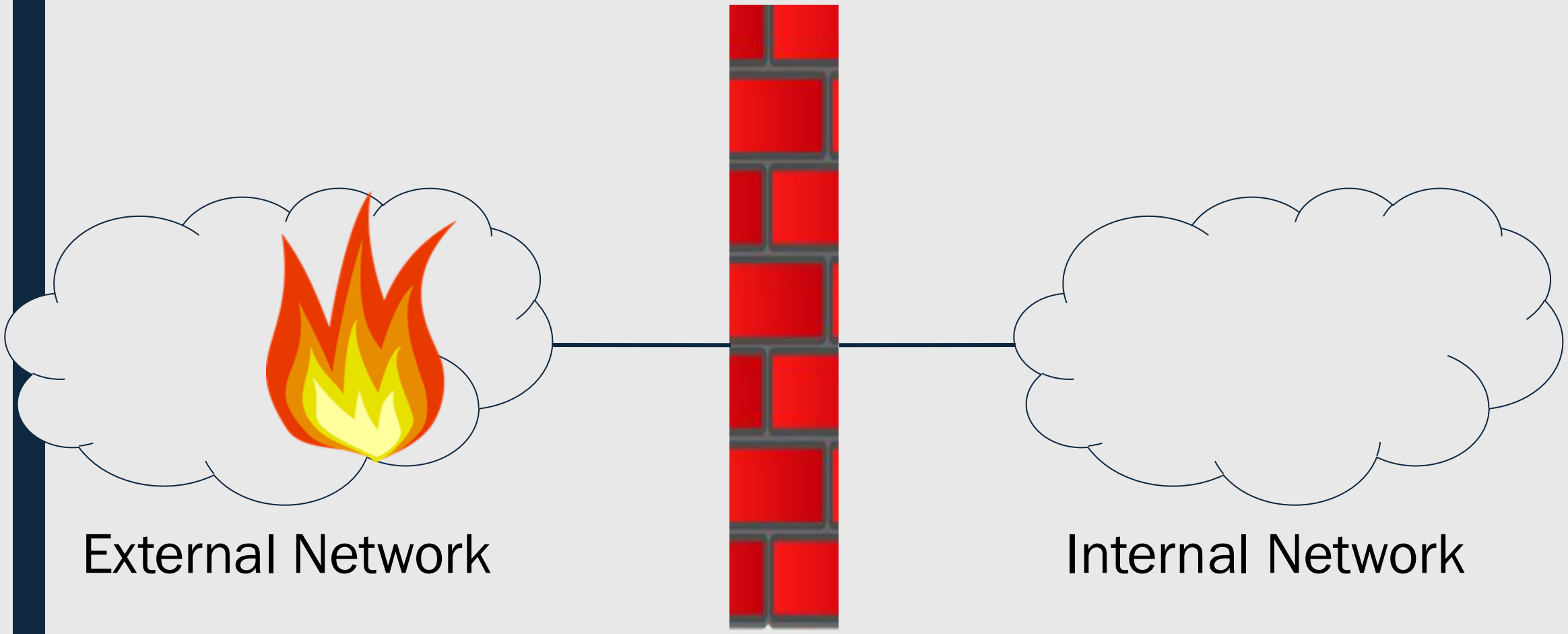
Intrusion Detection System

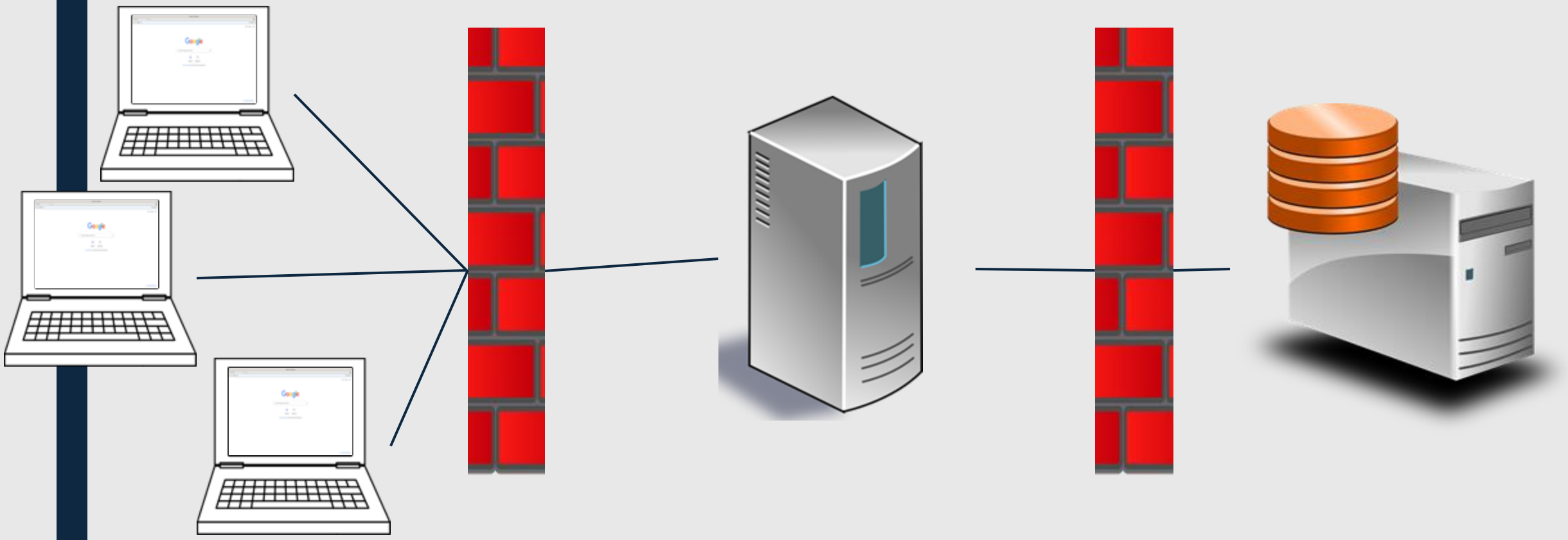


Tunnel



FIREWALLS


External Network
Internal Network



Internet

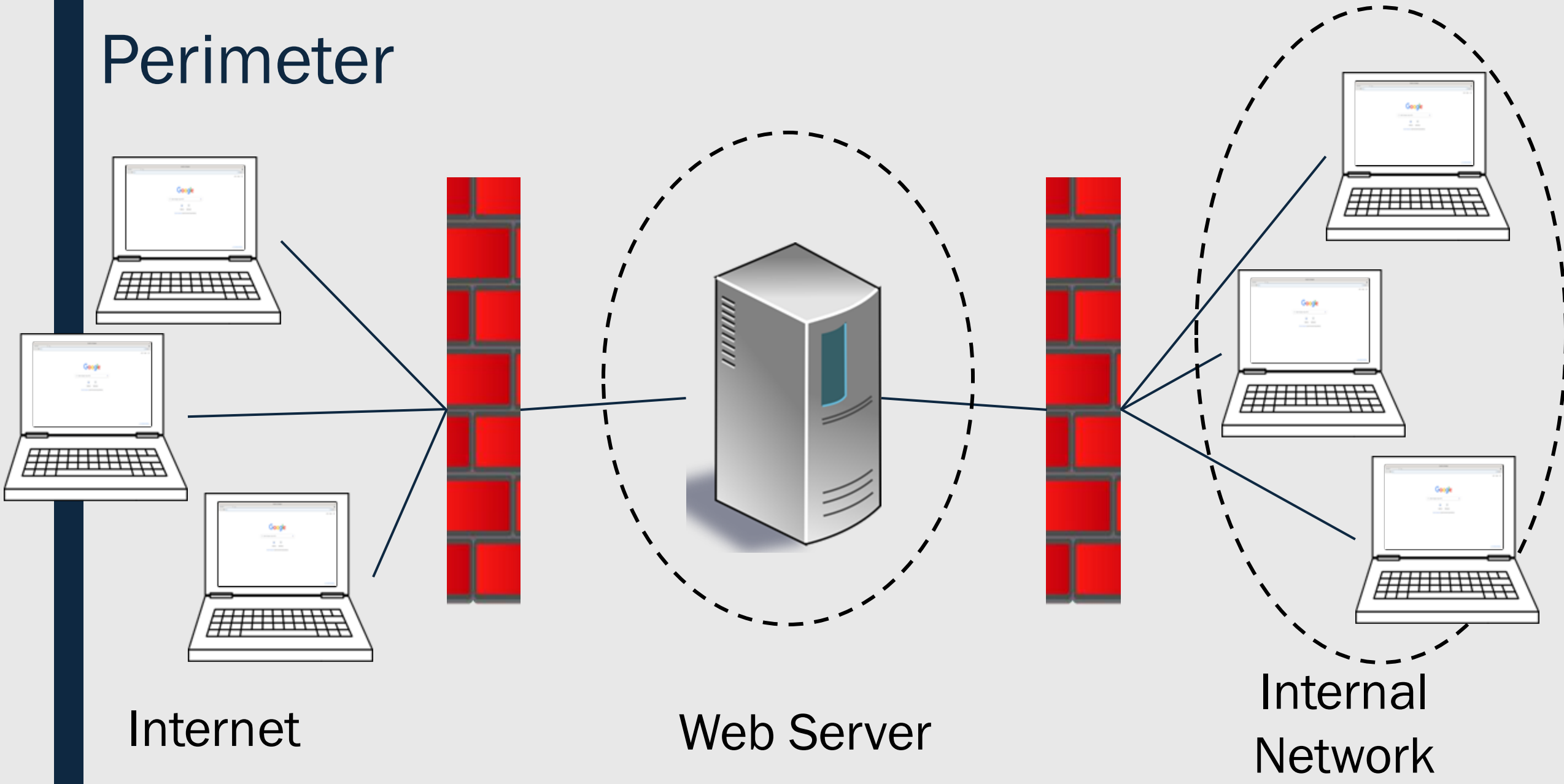
Web Server

Database Server

Firewall

Def’n: a gateway between two networks that can allow, deny, or modify data passing from one to the other

Perimeter



Firewall Properties

- security perimeter
- defense in depth: *used in conjunction w/ other methods*
- chokepoint for security analysis: *all communication funnels through*
- reference monitor
  - *complete mediation*
  - *immune to attack*
  - *proven correct*

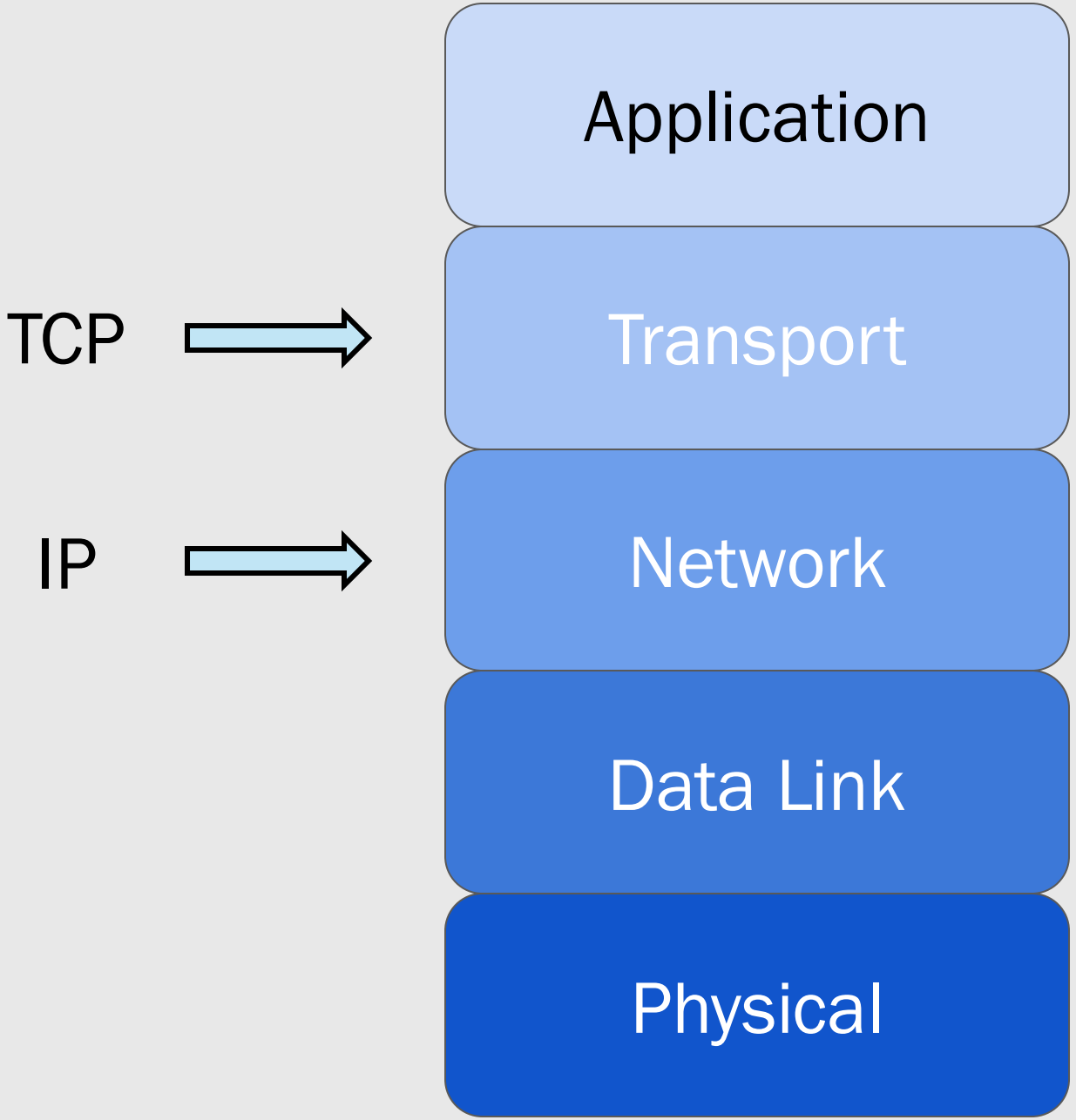
Types of Firewalls

Packet Filters

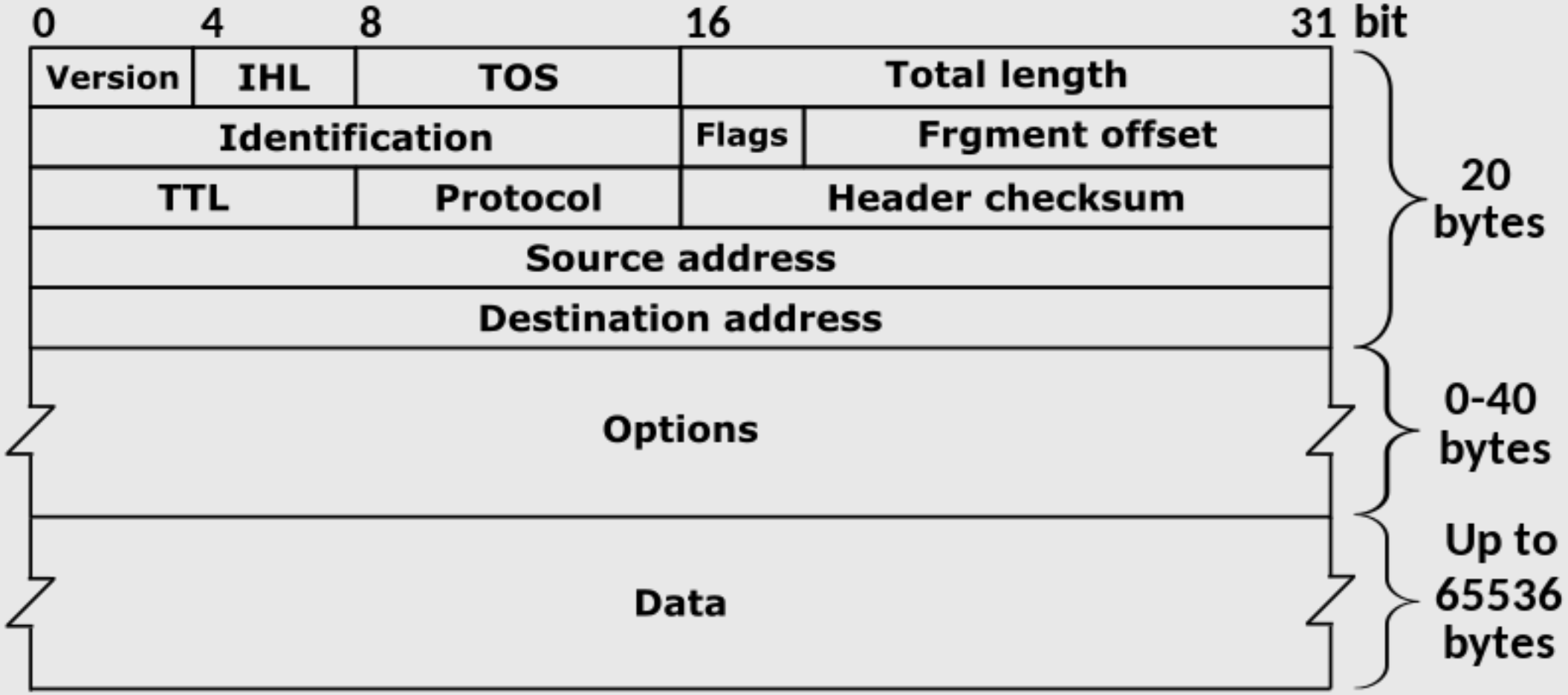
Proxy

FIRST, SOMEBACKGROUND: TCP/IP

TCP/IP

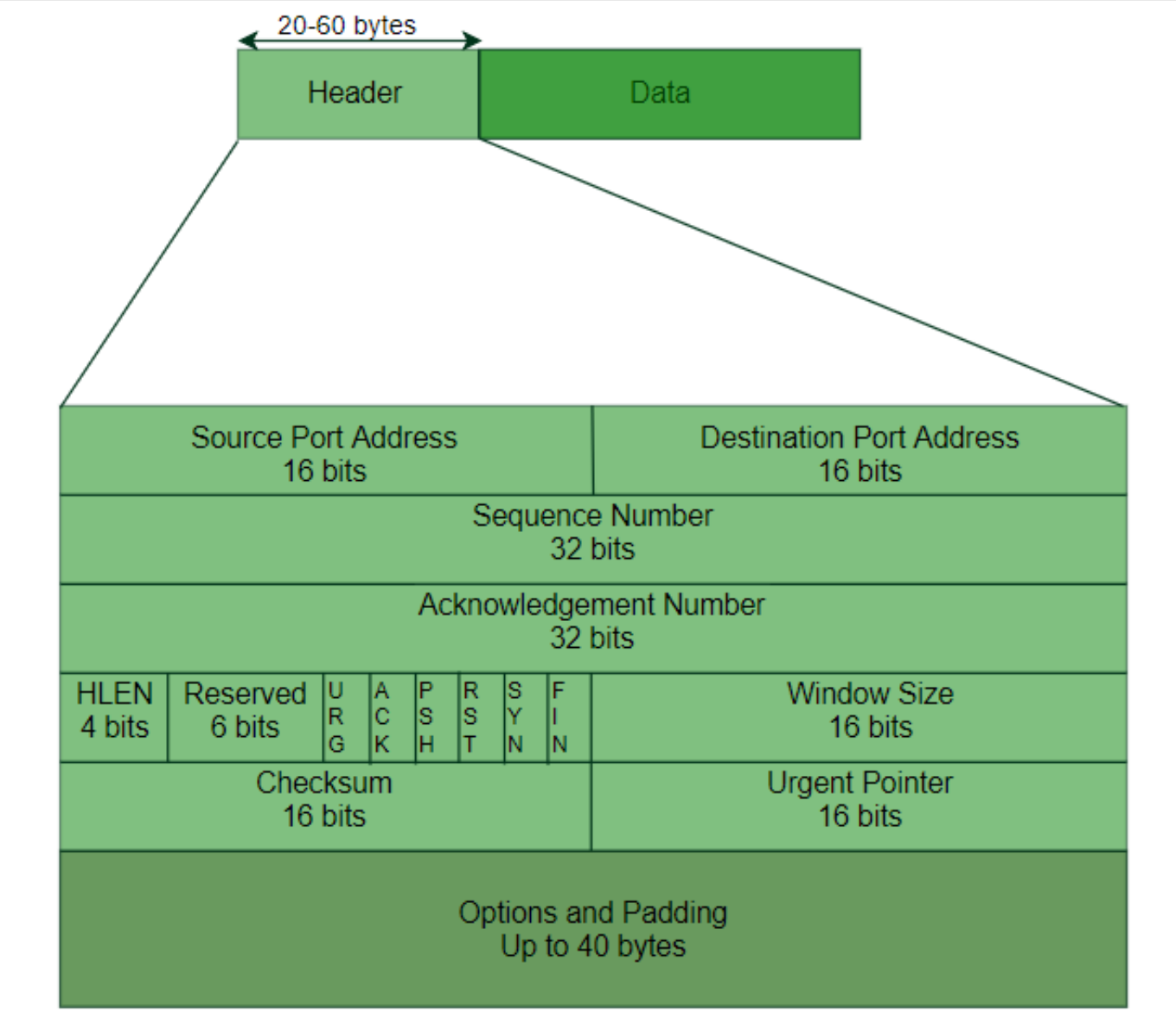


IPv4 Packet



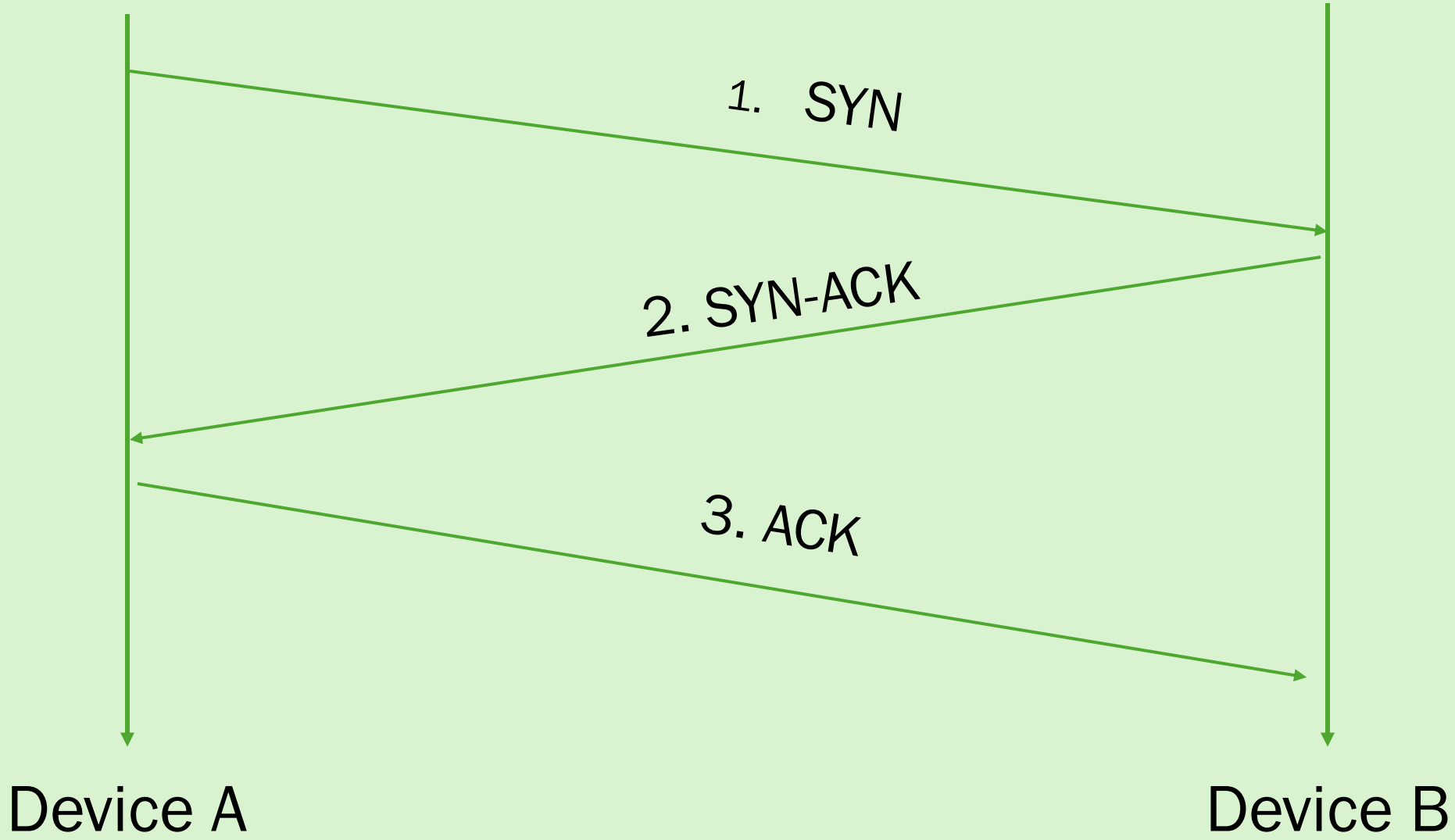
https://en.wikipedia.org/wiki/File:IPv4_Packet-en.svg

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

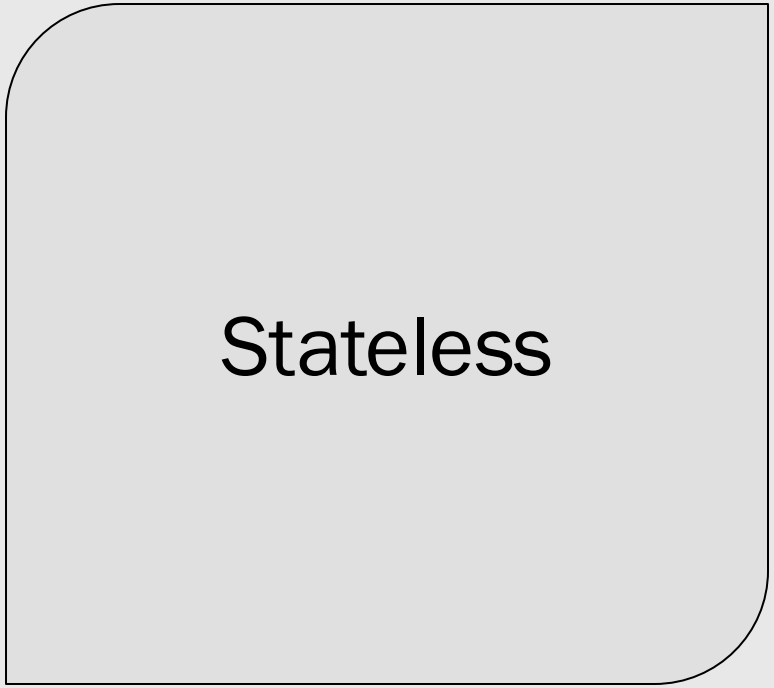
- TCP/IP header fields
- IP header protocol
- Packet size, flags
- Application protocol
- User ID
- Network activity

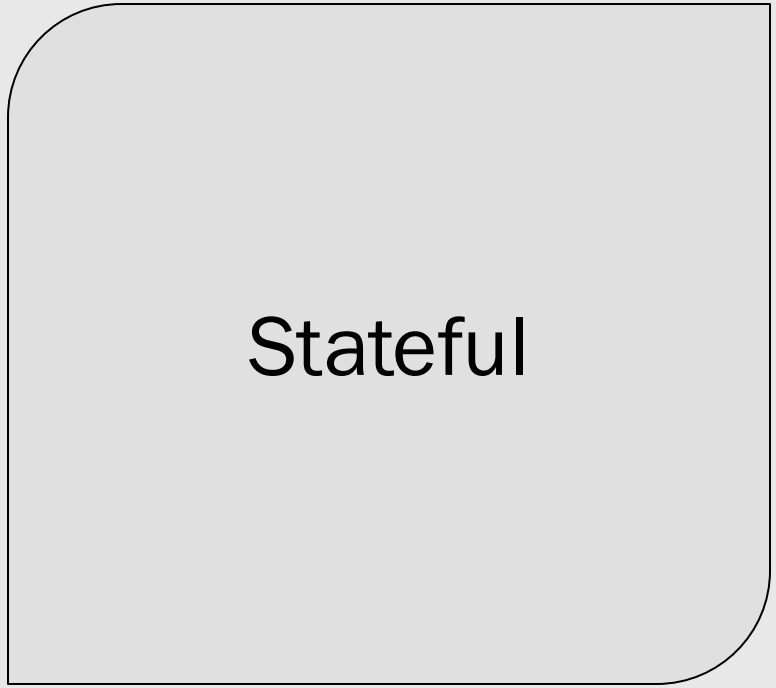
Packet Filters

Positive:
Default Deny

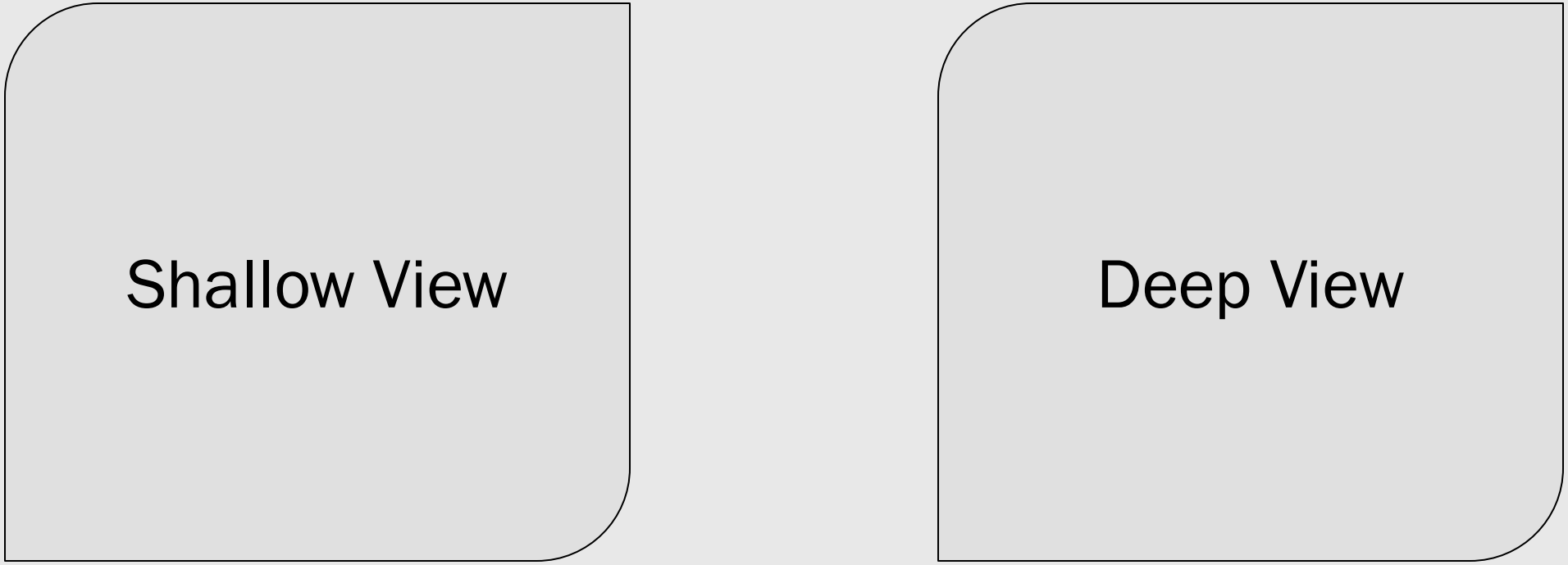
Negative: Default
Allow

Packet Filters





Packet Filters



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

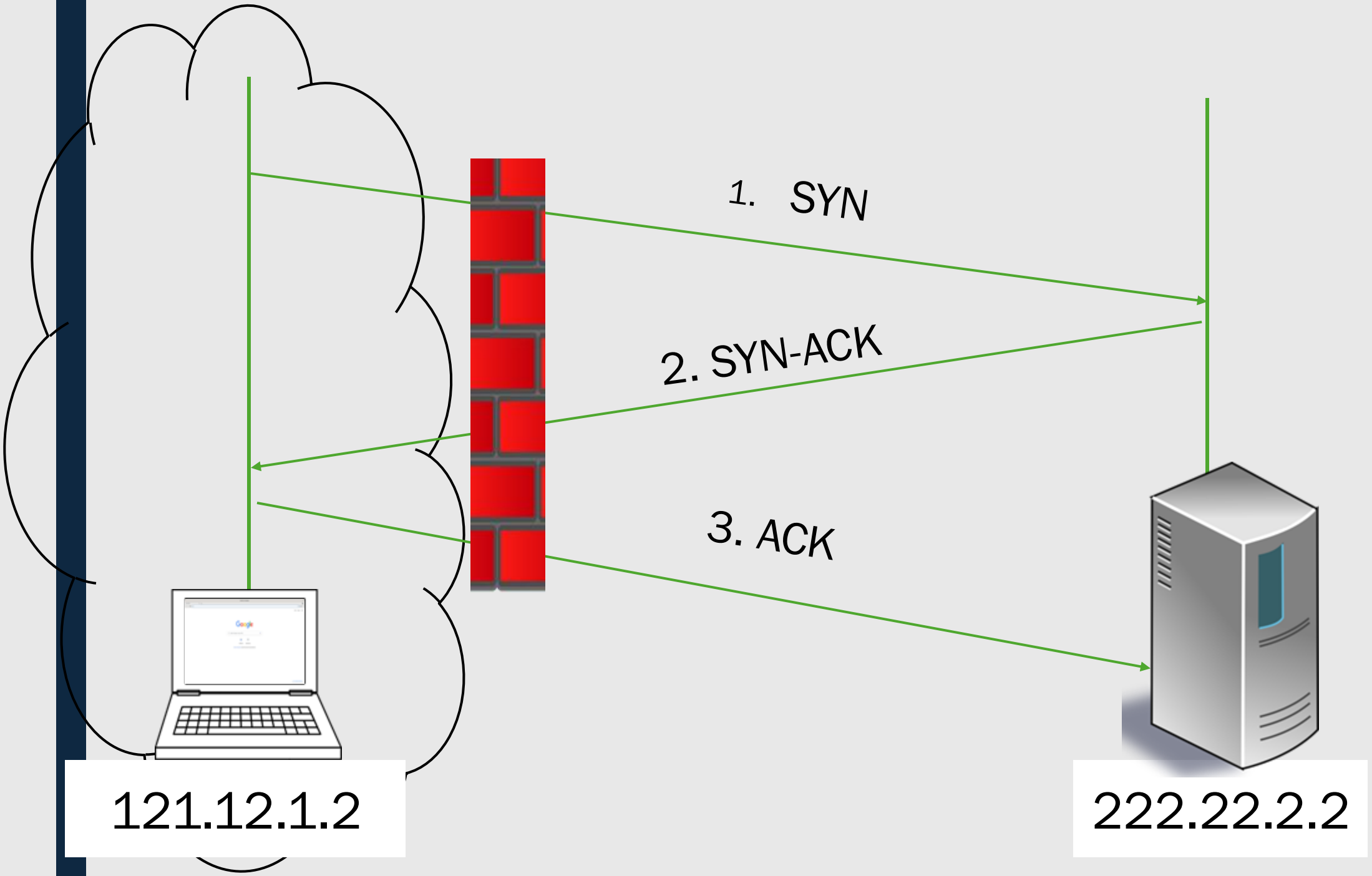
Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

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

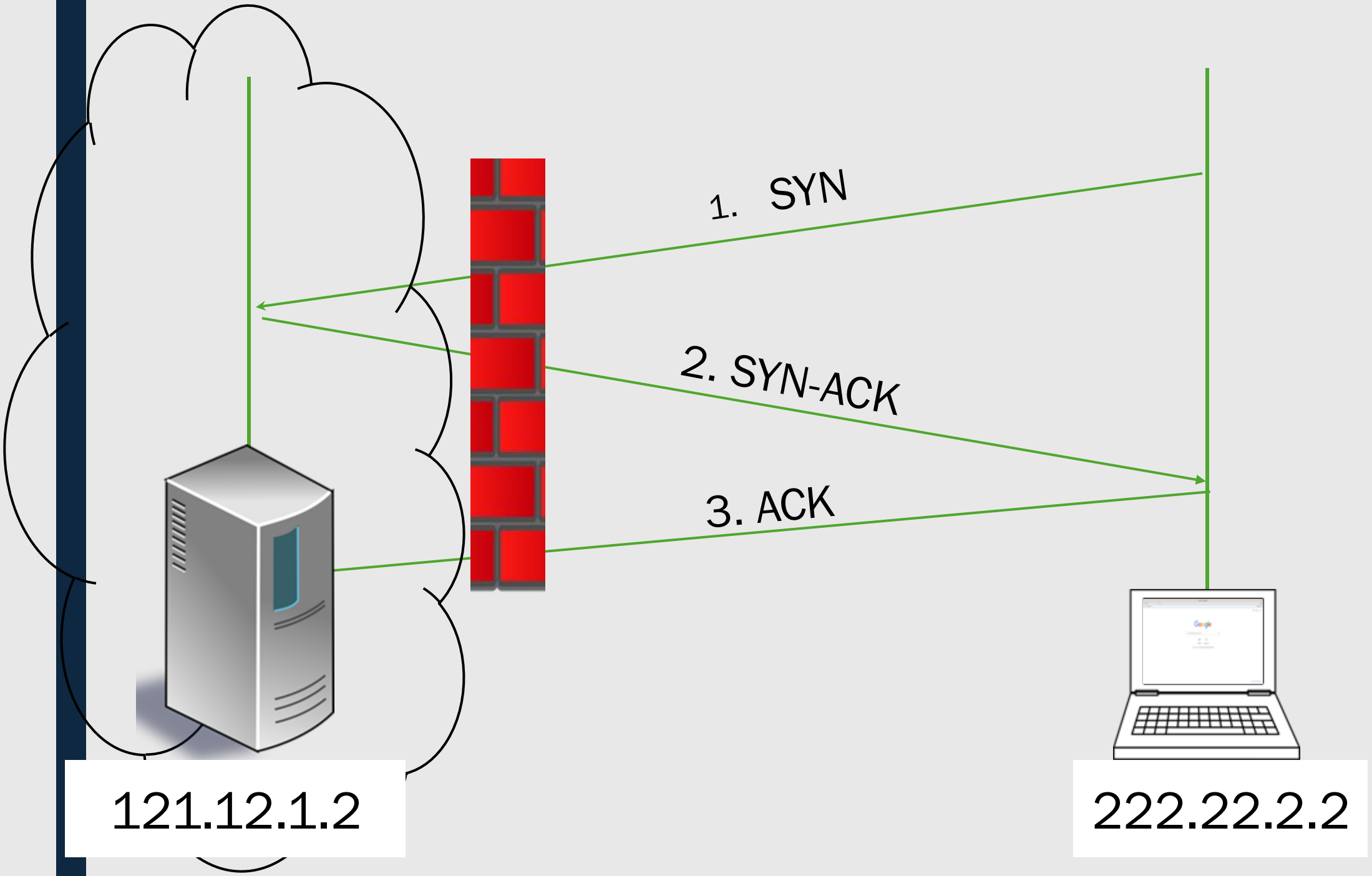
Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.


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

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)

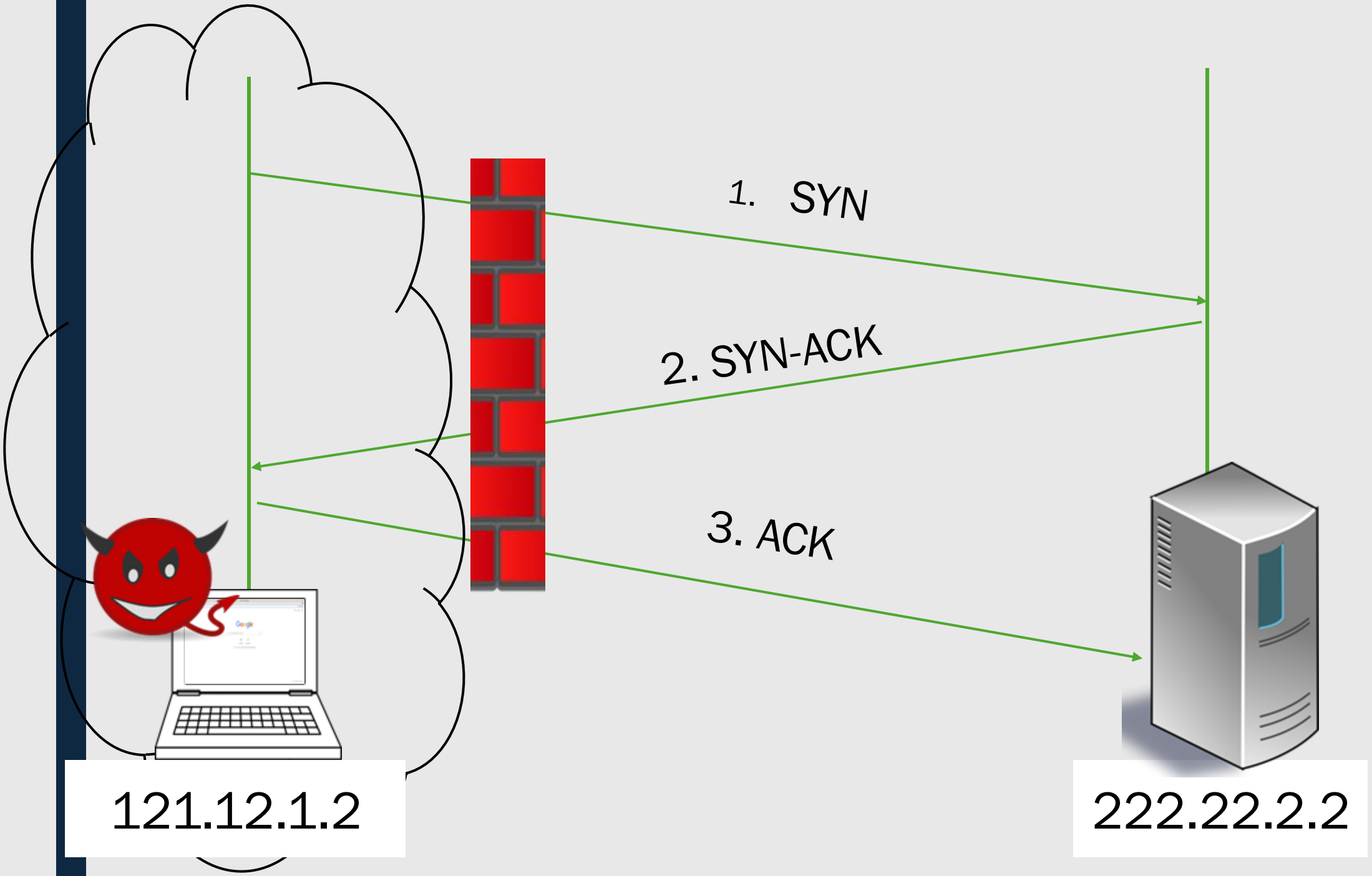
Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.


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

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)
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)

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


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

Rule	Dir	Src Addr	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

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

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

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

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)

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

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)

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

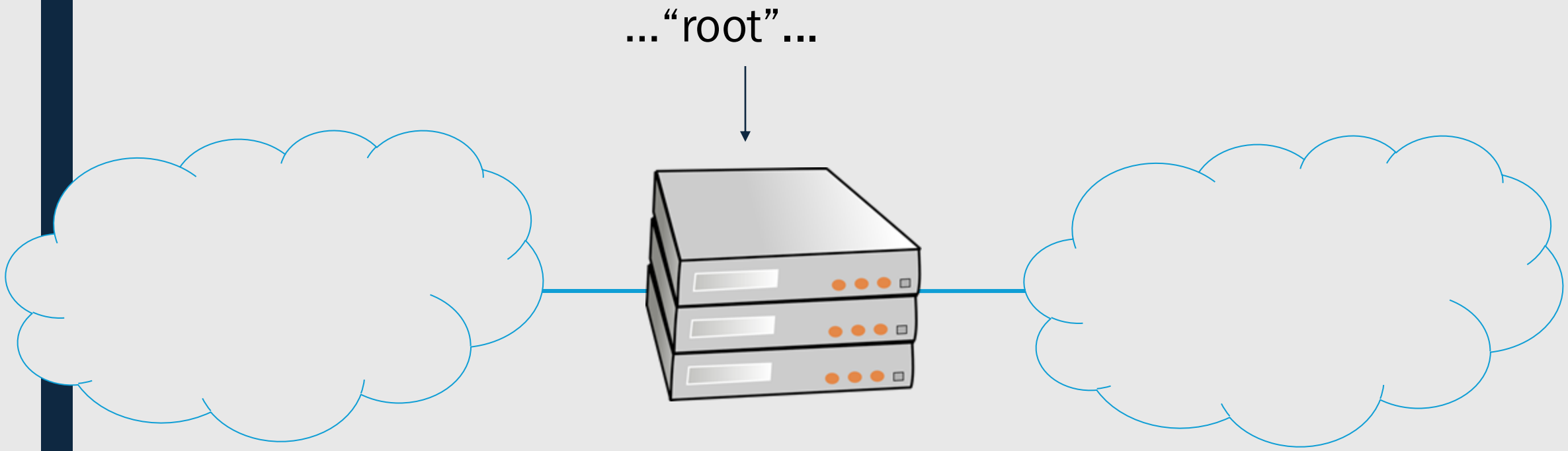
Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	25	8080	No	Deny (E)

Problem: packet filters have an imperfect view

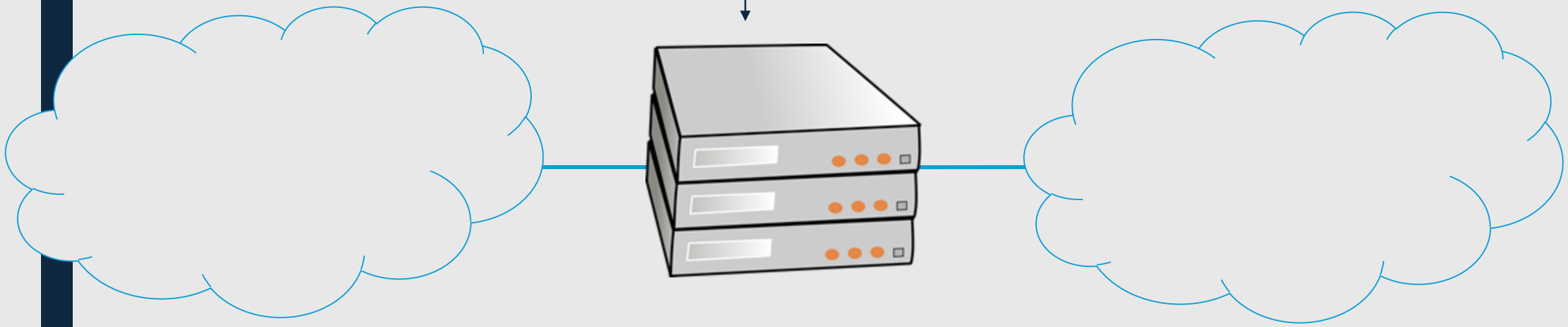
Signature-Based Filters

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

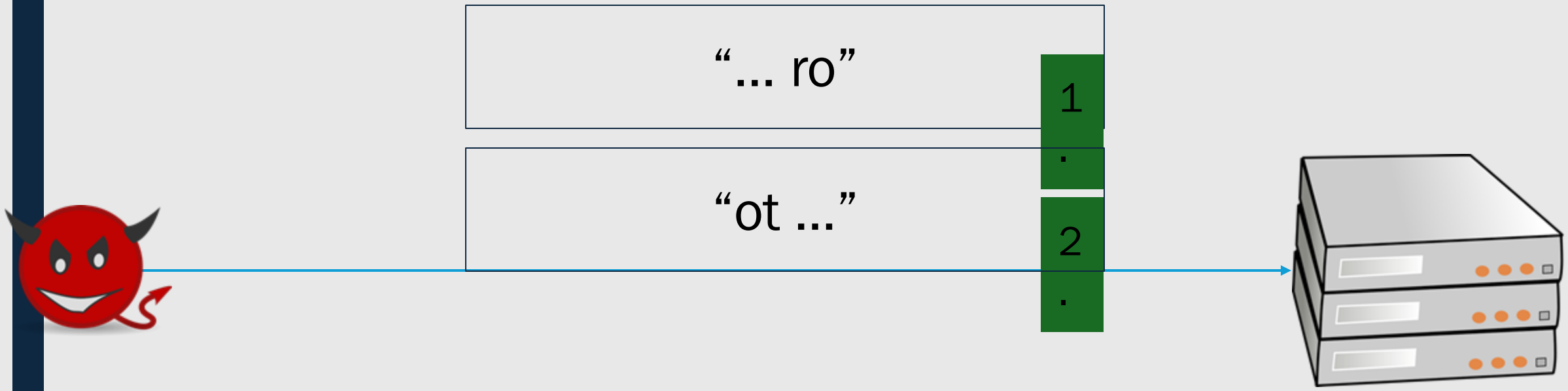
IP Header | TCP Header | “....root...”



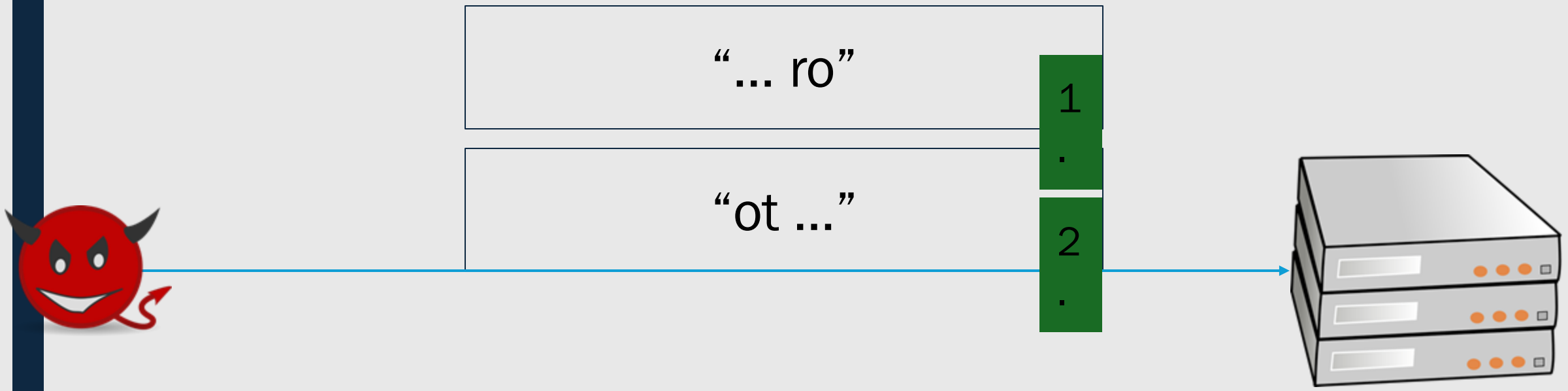
External Network

Internal Network

Attack



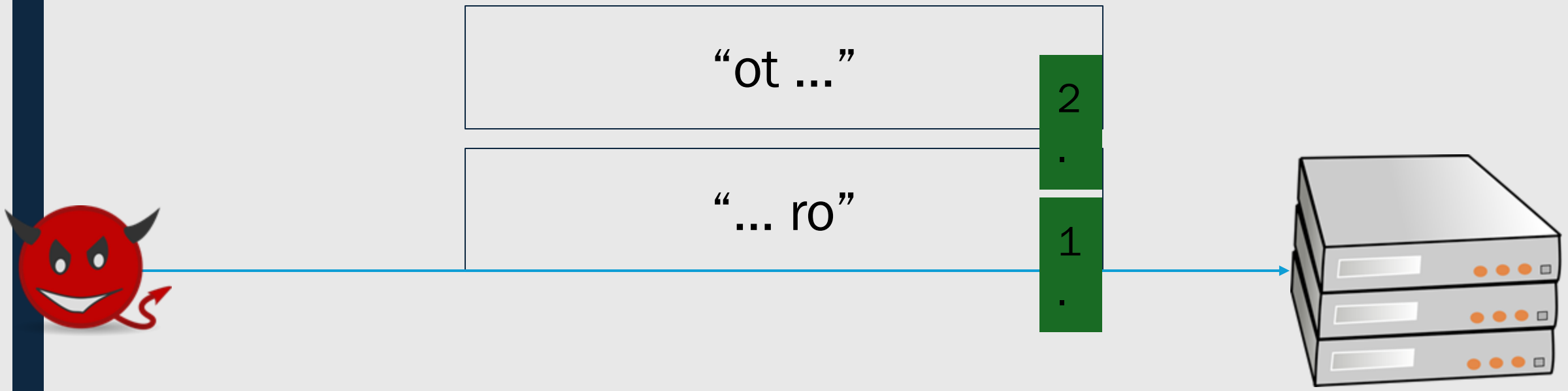
Attack



Fix: Track sequences of packets

Downside…. Have to track more state.

Attack



Attacker can easily ensure segments sent out of order.

Another Attack

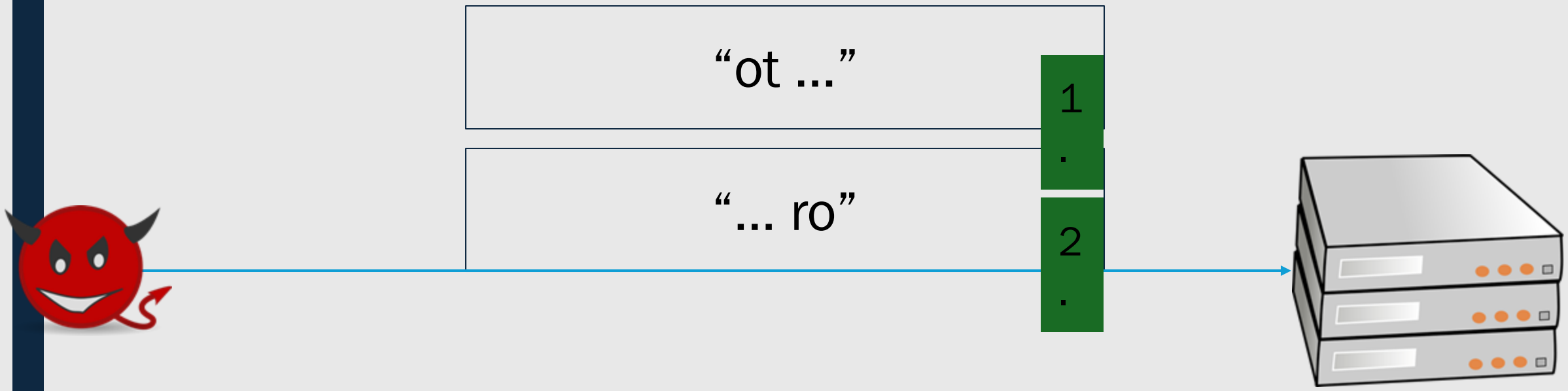
TTL=25	“r”
TTL=19	“i”
TTL=25	“o”
TTL=19	“p”
TTL=25	“o”
TTL=25	“t”

r

o

o

t



Fix: Reassemble the TCP stream