COMP435: *SECURITY CONCEPTS!*

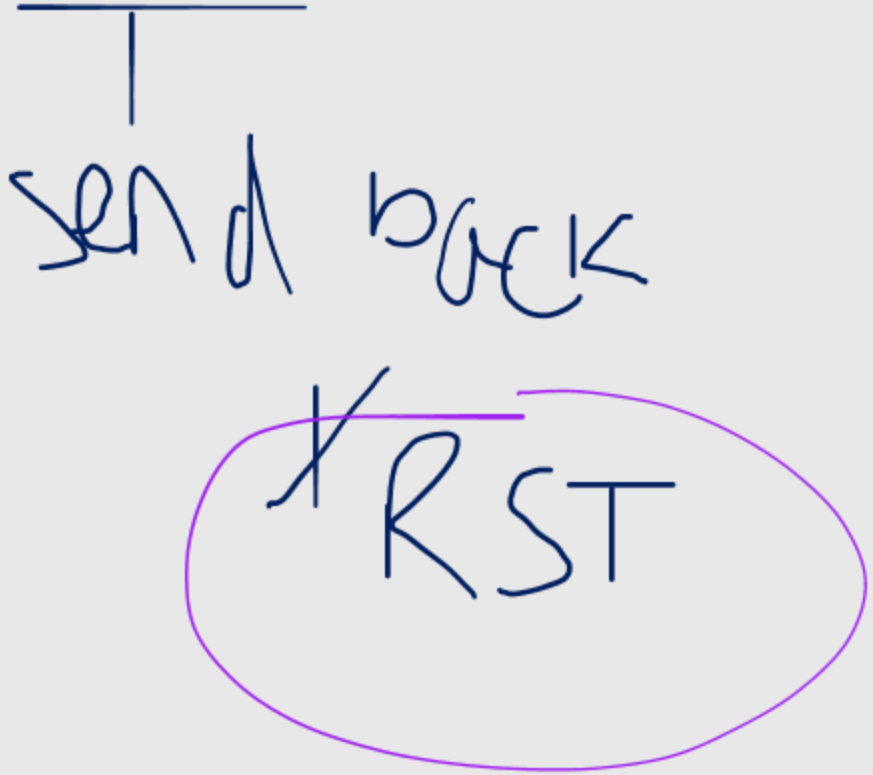
Lecture 18: Packet Filters

tinyurl.com/comp435-fa25

PACKET FILTERS

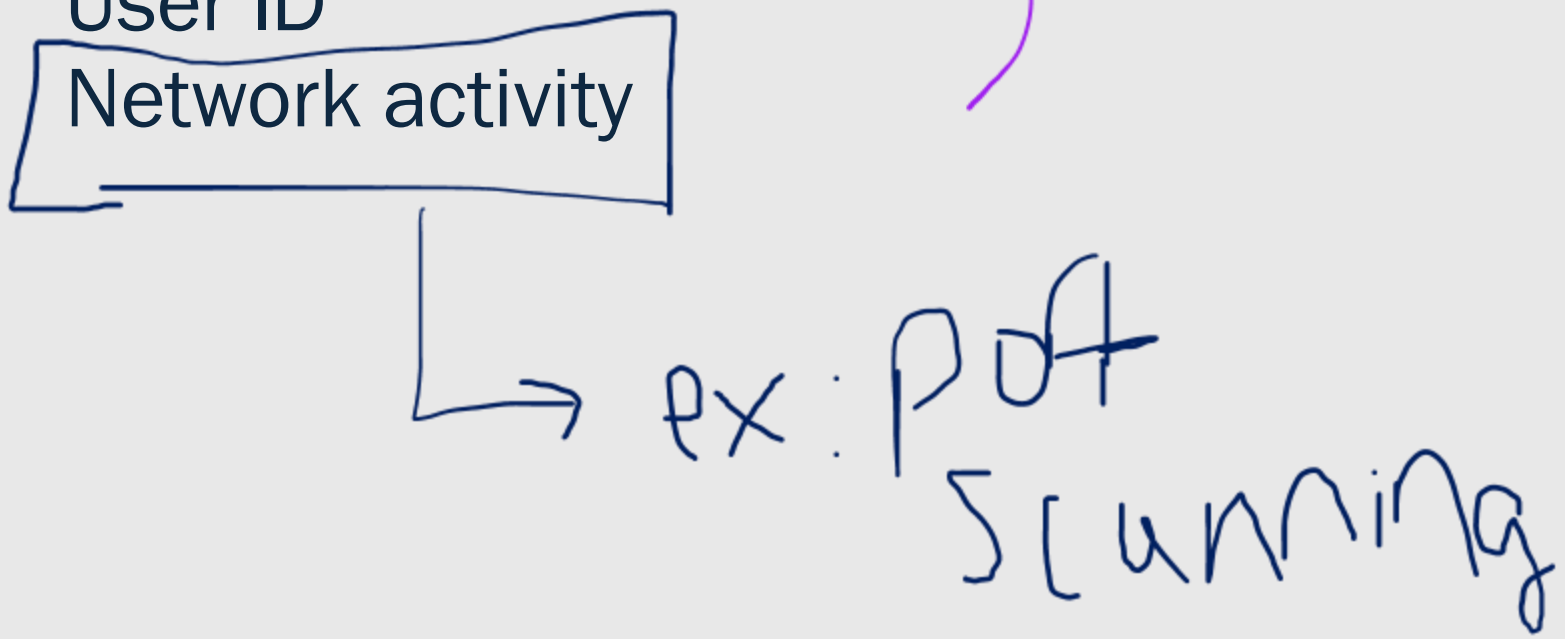
Packet Filter

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

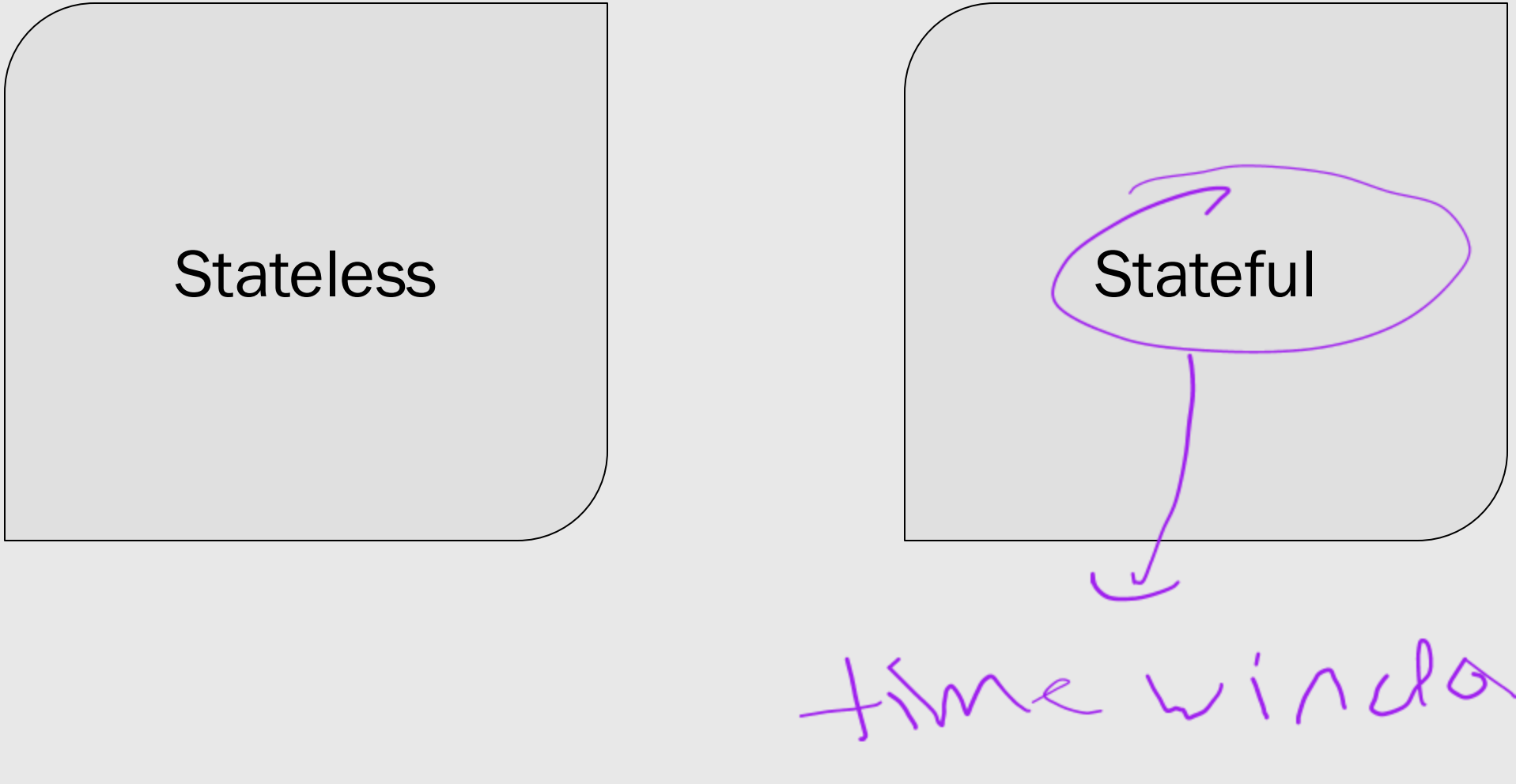


Packet Filters

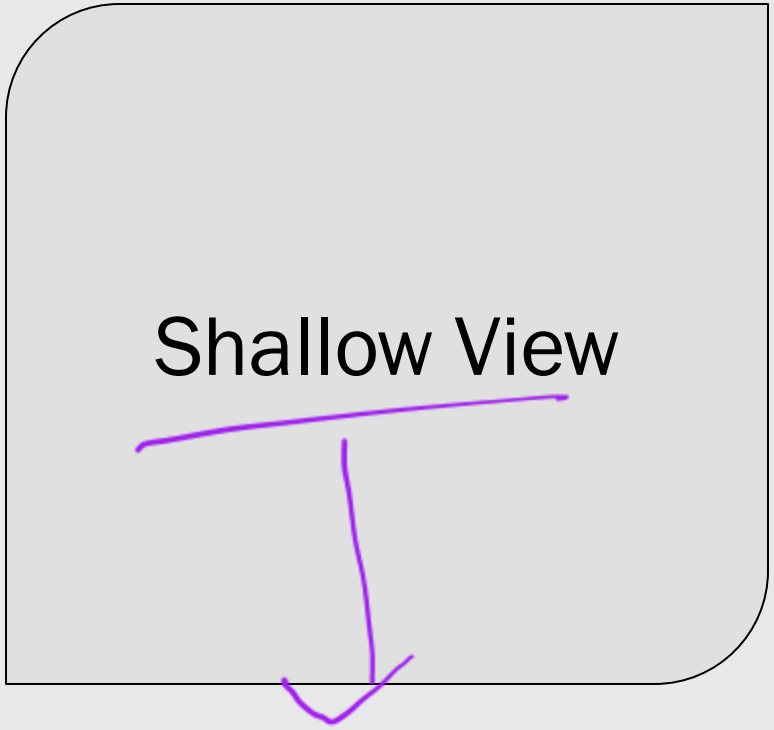
Positive: Default Deny

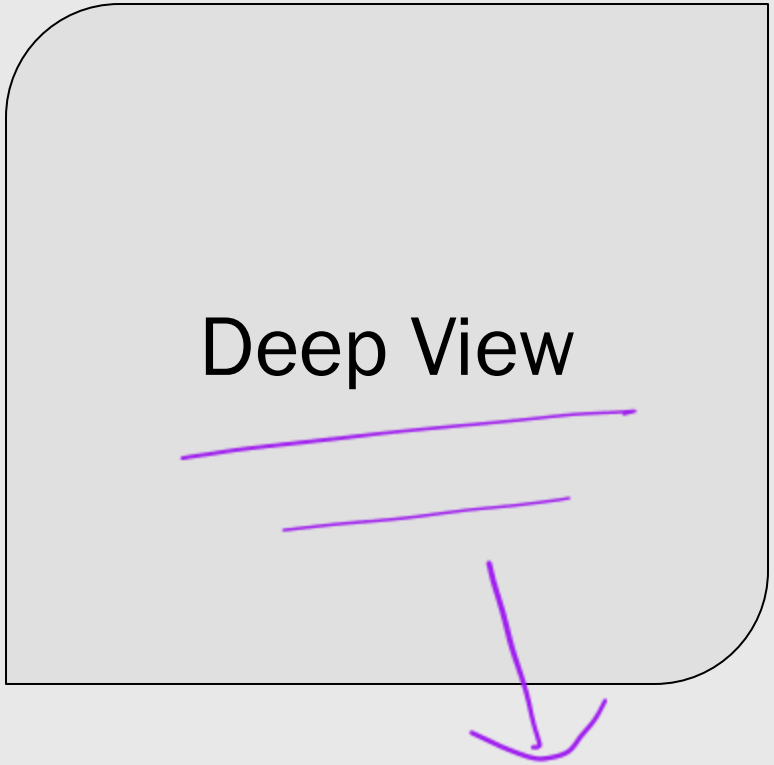
Negative: Default Allow

Packet Filters



Packet Filters





header only

payload / data

Firewall Limitations

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

An Example Packet Filter

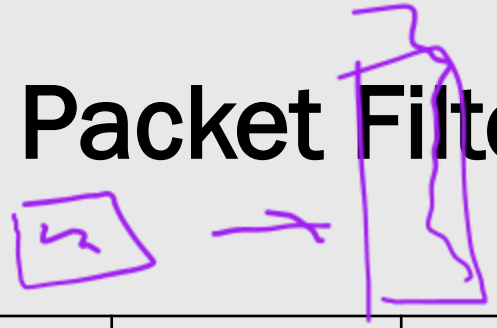
SMTP, or Simple Mail Transfer Protocol. Listens on Port 25

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

UDP, & ICMP

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

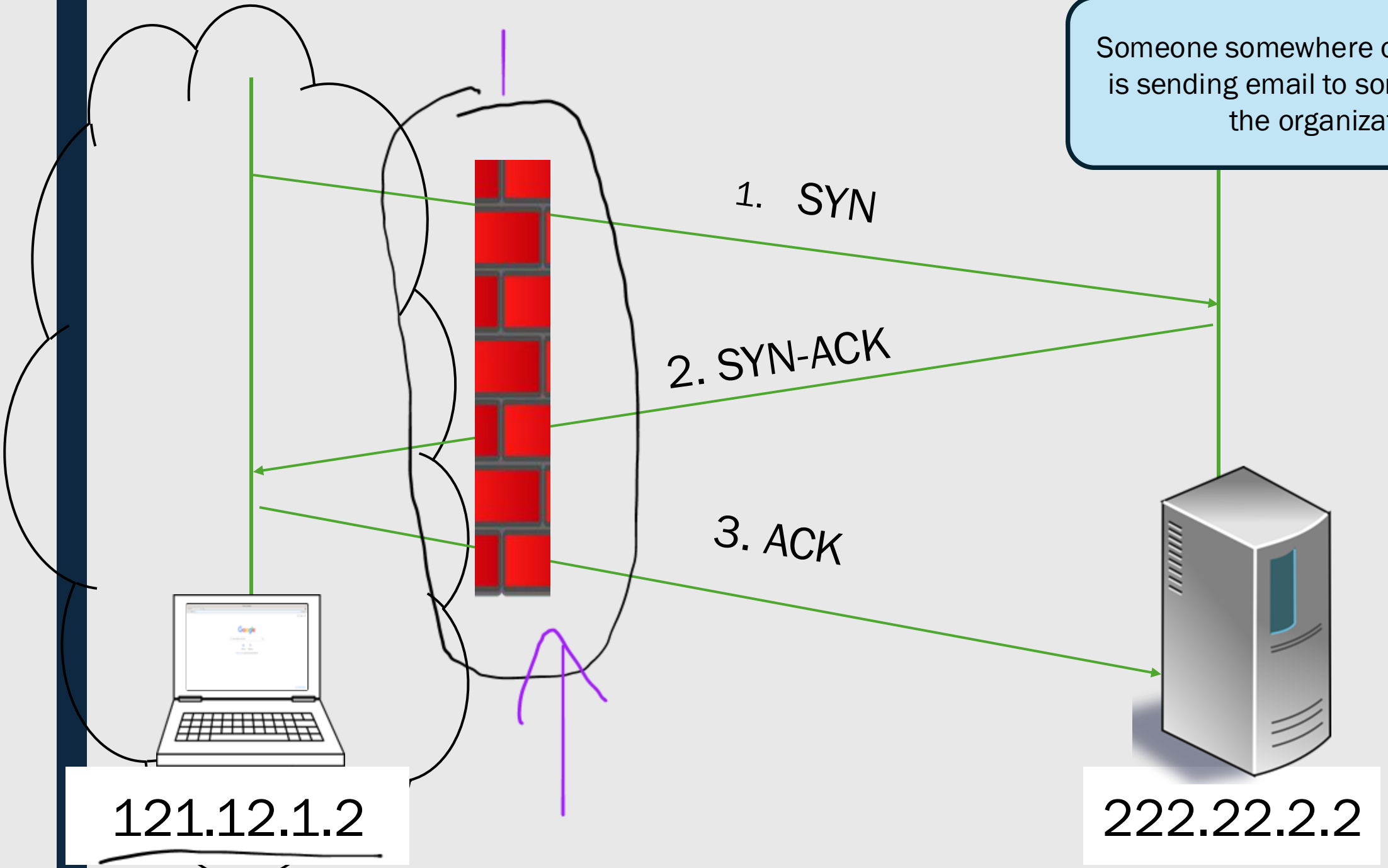
Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

An Example Packet Filter

Default deny!

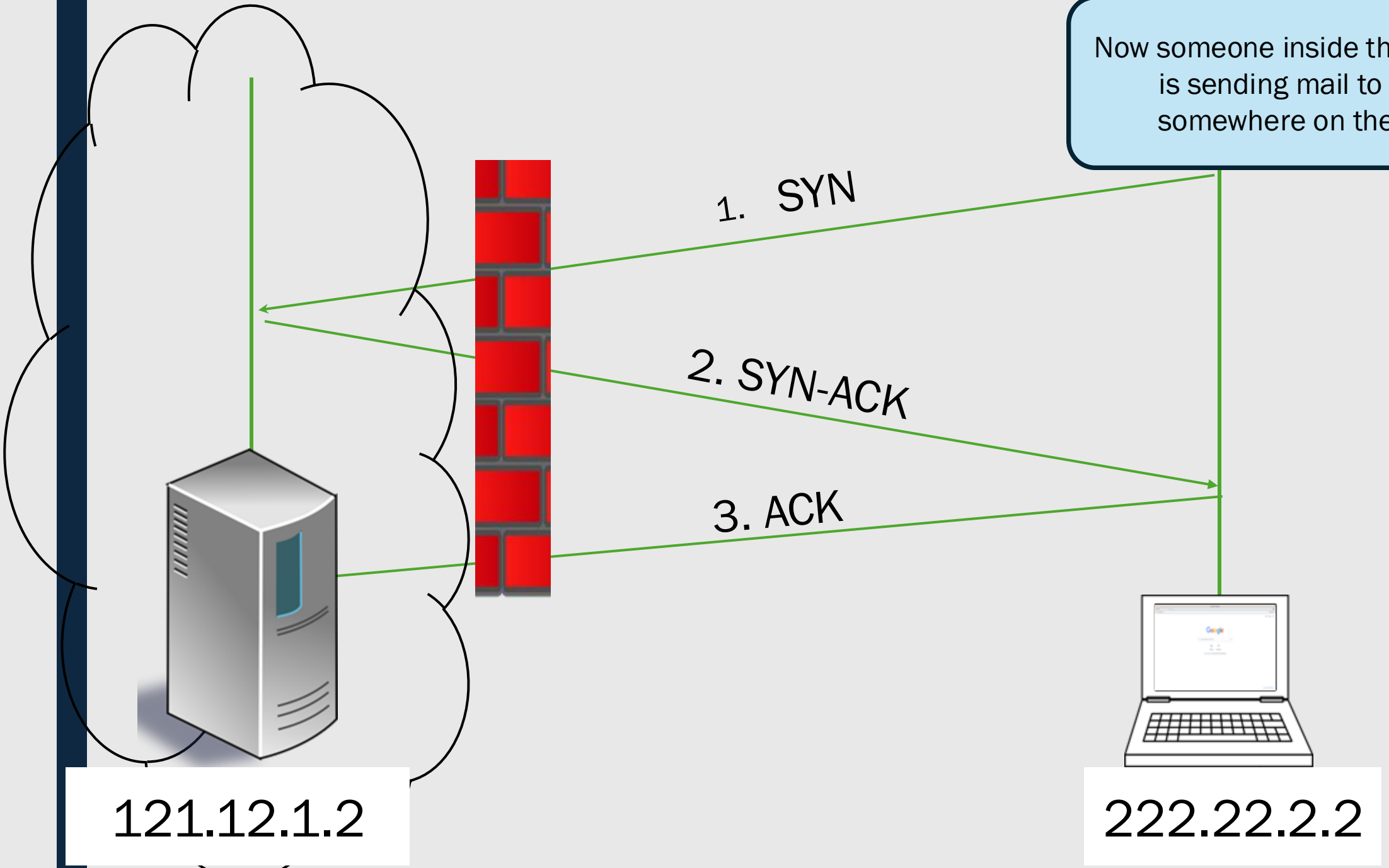
Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Allow
B	Out	Internal	External	TCP	>1023	Allow
C	Out	Internal	External	TCP	25	Allow
D	In	External	Internal	TCP	>1023	Allow
E	Either	Any	Any	Any	Any	Deny

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


Someone somewhere on the internet is sending email to someone inside the organization
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

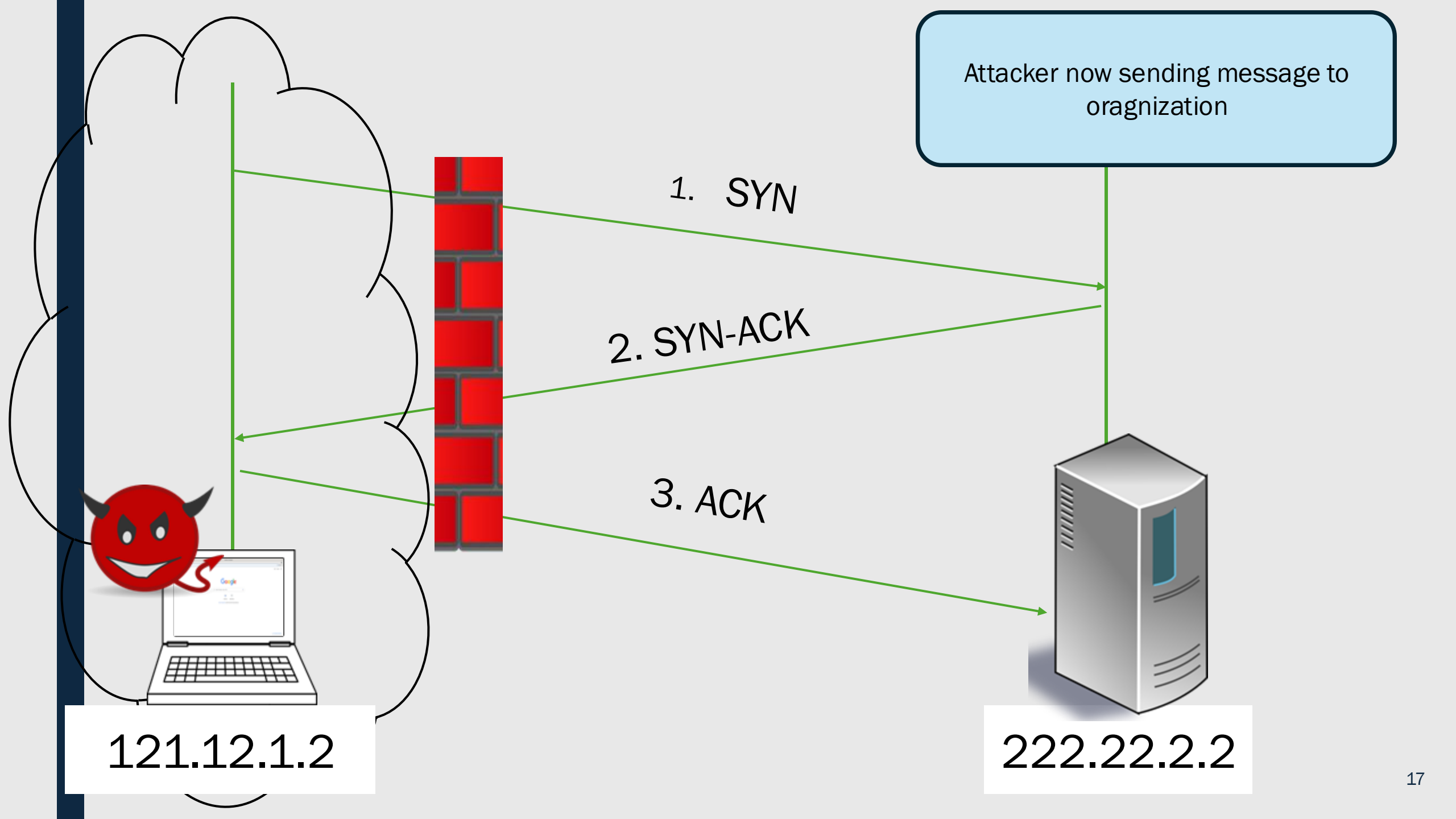
Packet	Direction	Src	Dest	Protocol	Dest Port	Action (rule)
1	In	121.12.1.2	222.2.2.2	TCP	25	Allow (A)
2	Out	222.2.2.2	121.12.1.2	TCP	5150	Allow (B)


Now someone inside the organization is sending mail to someone somewhere on the internet.
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	Allow (C)
4	In	121.12.1.2	222.22.2.2	TCP	5150	Allow (D)

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


Attacker now sending message to oragnization
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	D

Packet	Direction	Src	Dest	Protocol	Dest Port	A (r
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)

Attacker starts web proxy server on port 8080… packet filter allows this connection! ☹

Rule	Dir	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B						
C						
D						
E						

The packet filter assumed rules A and B would be used together and rules C and D would be used together.

An attacker is not bound by any such assumption and here, the TCP connection is making use of rules D and B together.

r starts web
rver on port
packet filter
ows this
nection! ☹

Packet						
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	

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	De	
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)

Another attacker: starts communication from SMTP server and gets response from proxy server!

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

There is some implicit ordering in the rules. The expectation is that rule C will be applied first -- to an outgoing packet initiating a connection -- and then rule D would be applied to the resulting response packets.

That ordering is not enforced and in this attack, it is rule D that gets applied first to an incoming packet initiating a connection

starts
m SMTP
sponse
ver!

Packet							
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			ACK Set	Action
A	In	External	Internal	TC			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

The ACK flag is only set in response to another message. Including it in the rules stops this attack.

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	?? (?)

Allow D

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)
2	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	5051	25	Yes	?? (?)

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	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)
3	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	25	5055	Yes	?? (?)

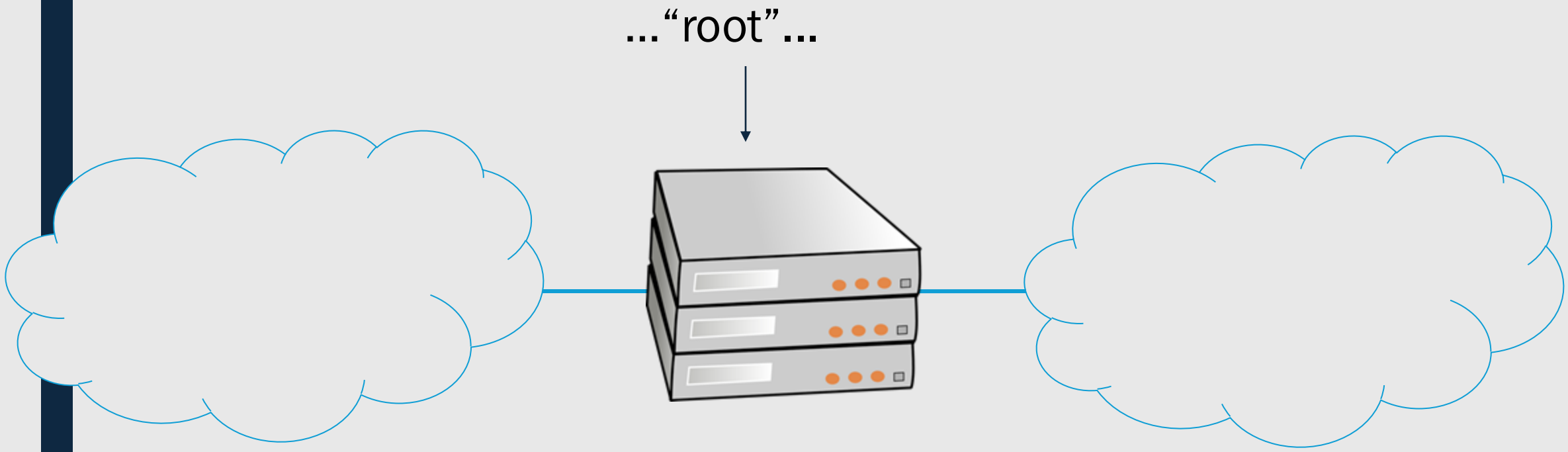
Building Internet Firewalls: Internet and Web Security, by Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, ch. 8.

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

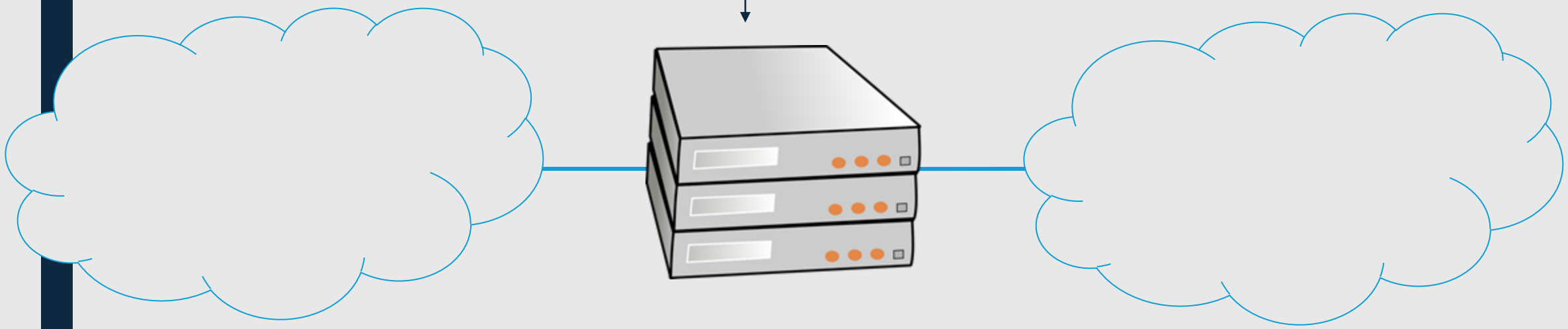
E.g., look for “root”; look for “/etc/passwd”



External Network

Internal Network

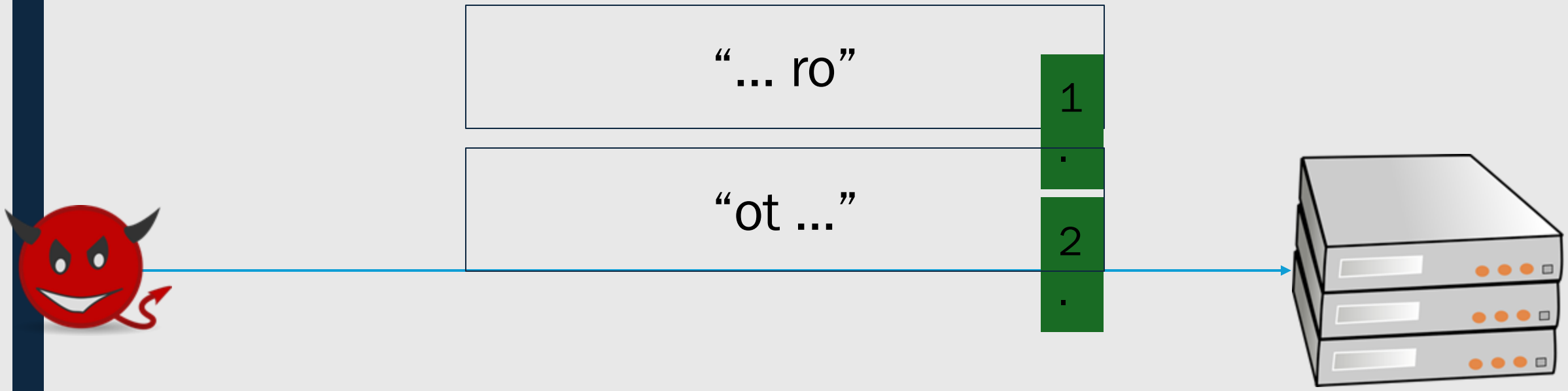
IP Header | TCP Header | “....root...”



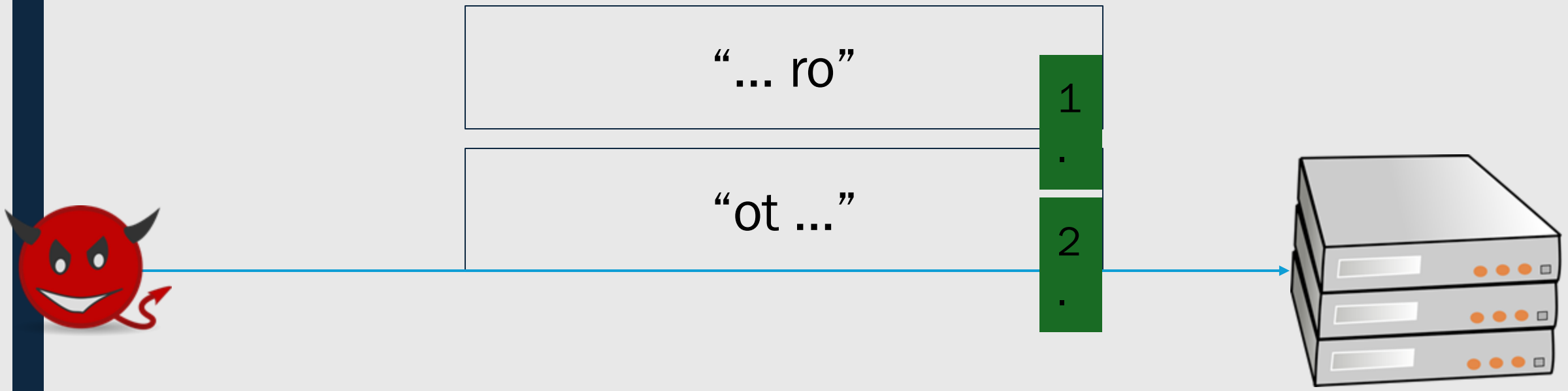
External Network

Internal Network

Attack



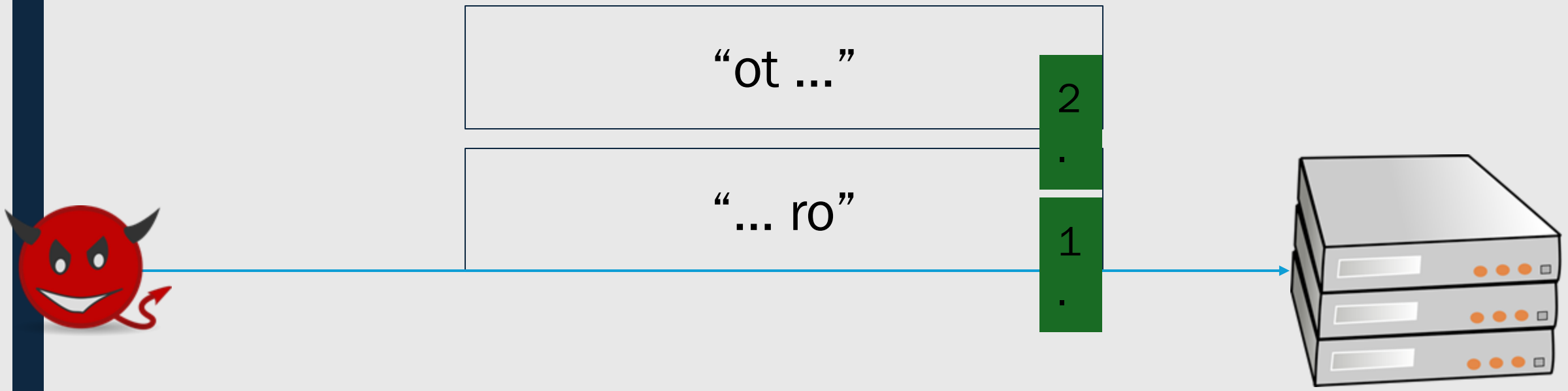
Attack



Fix: Track sequences of packets

Downside…. Have to track more state.

Attack



Attacker can easily ensure segments sent out of order.

Another Attack

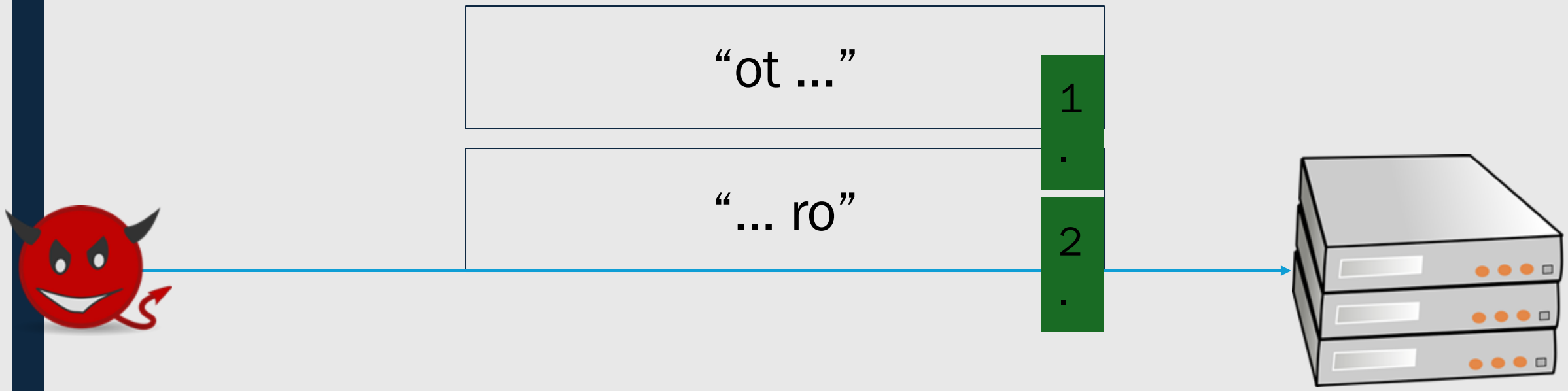
TTL=25	“r”
TTL=19	“i”
TTL=25	“o”
TTL=19	“p”
TTL=25	“o”
TTL=25	“t”

r

o

o

t



Fix: Reassemble the TCP stream