February 1, 2021
Edge Protection

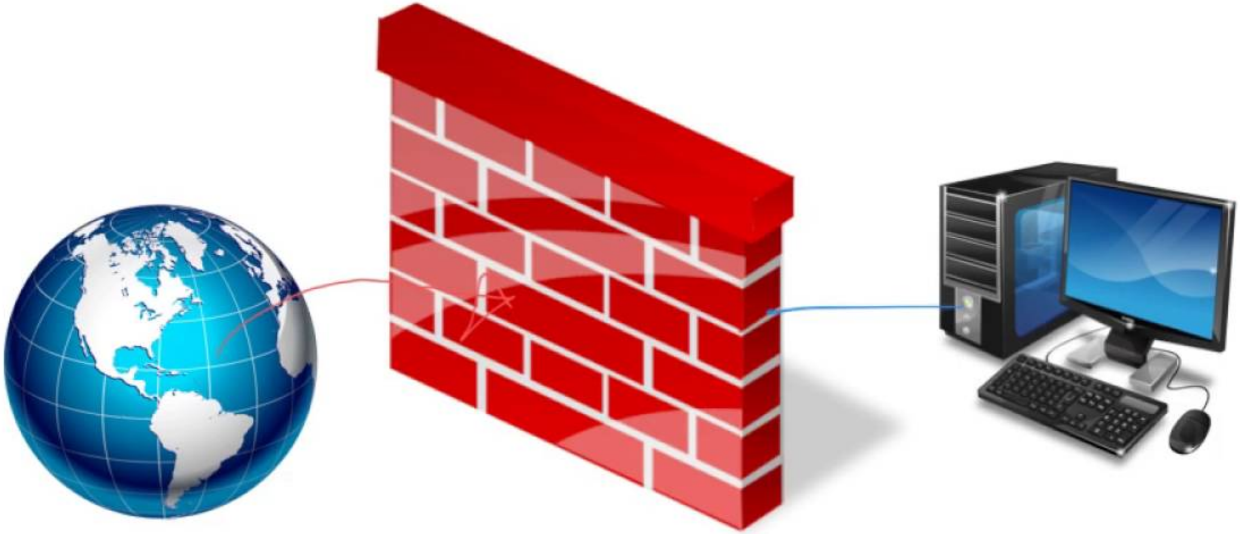
COLLEGE of CHARLESTON 1770

- Assignments
  - Lab 1: Due Monday, Feb 22
  - Project
    - Topic Due: Monday, Feb 22

Research

- Sources
    - scholar.google.com
    - CofC Library
- Citation Chains
- Organized Approach to Research
    - Papers (tooling)
    - Experimental results

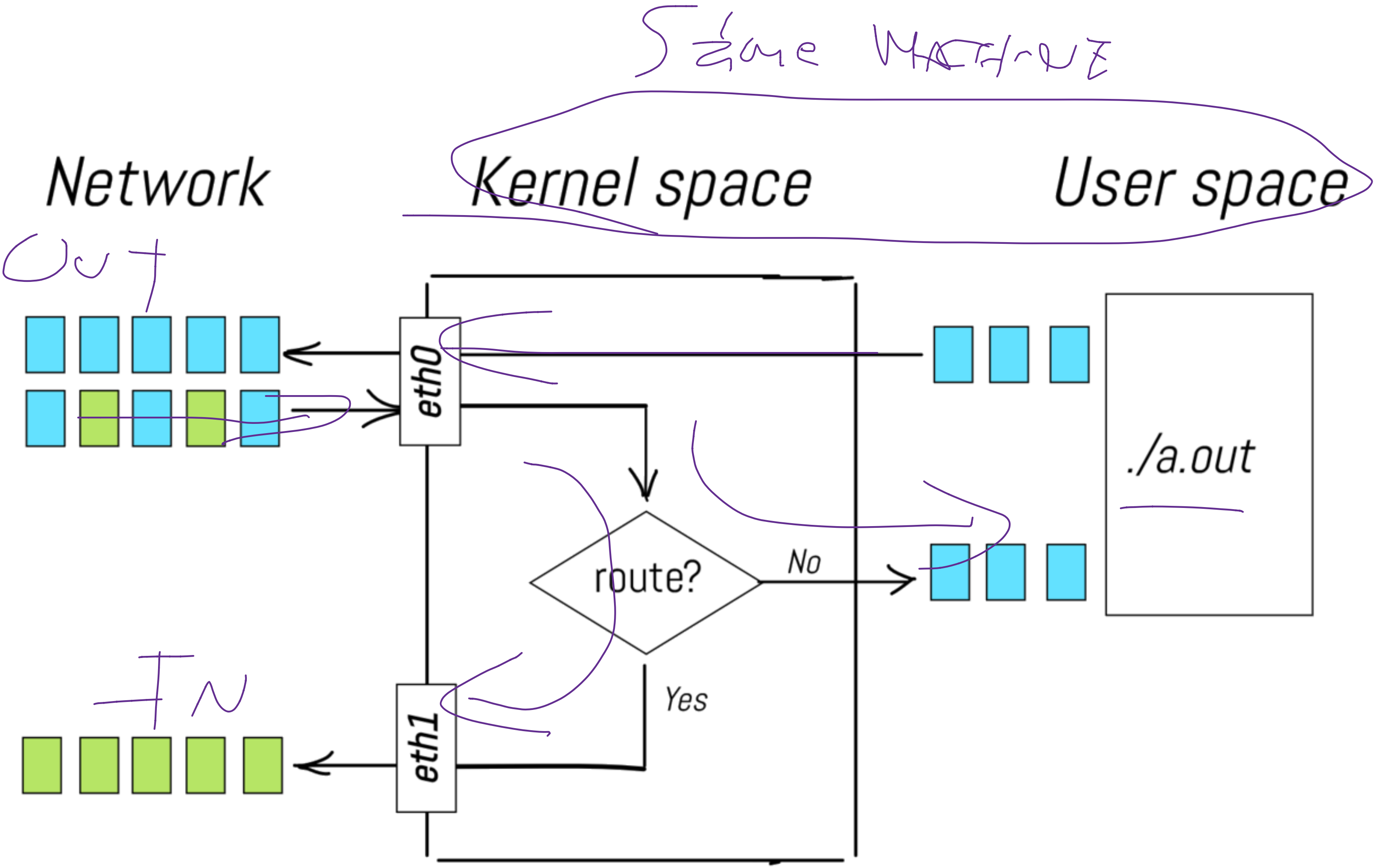
iptables



FIREWALLS

- Rules for inbound/outbound ACCESS TO NETWORK
- Logging ACTIVITY
- PORT FORWARDING
- NAT NETWORK Address TRANSLATION

Same MACHINE



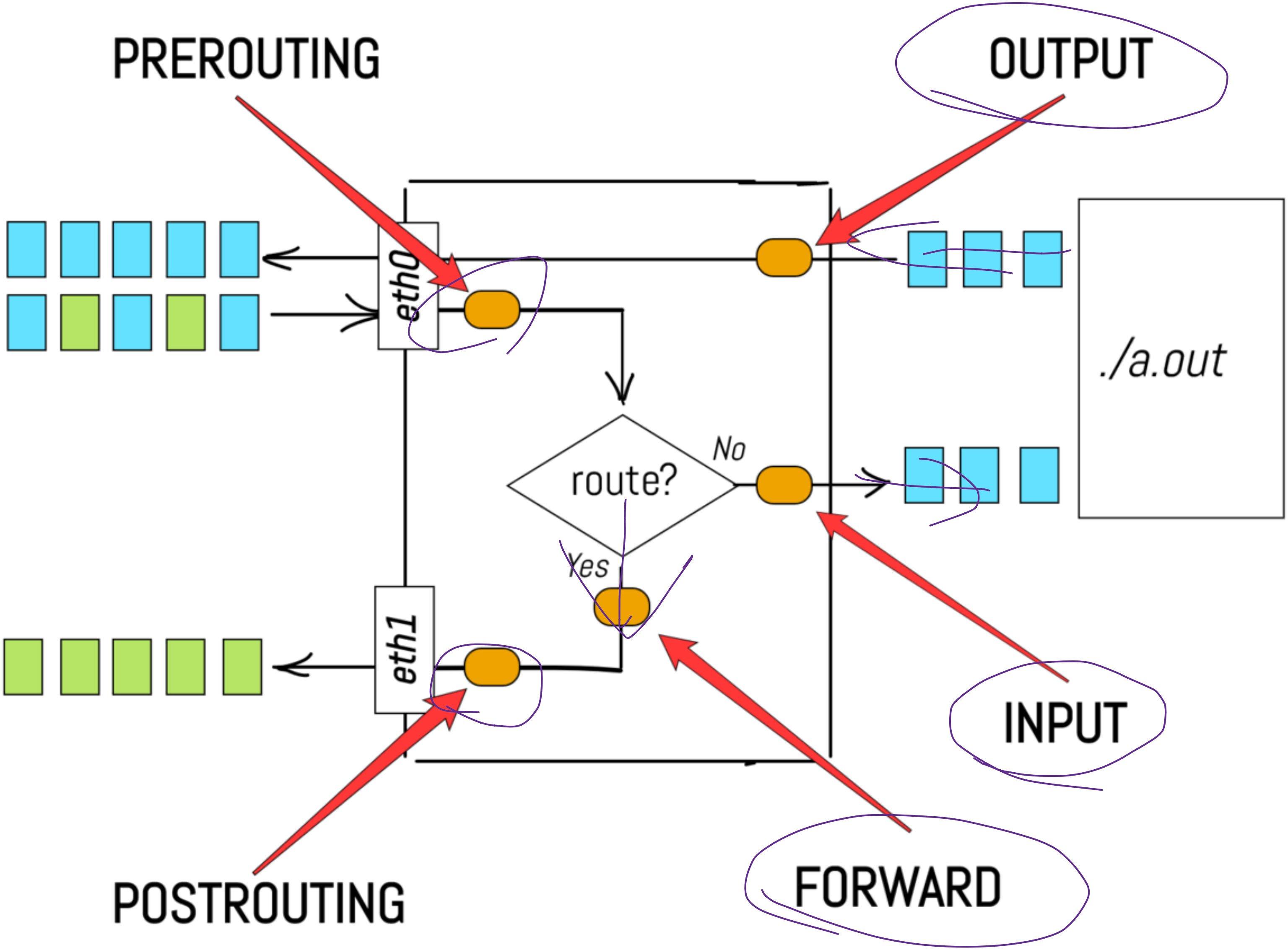
Network

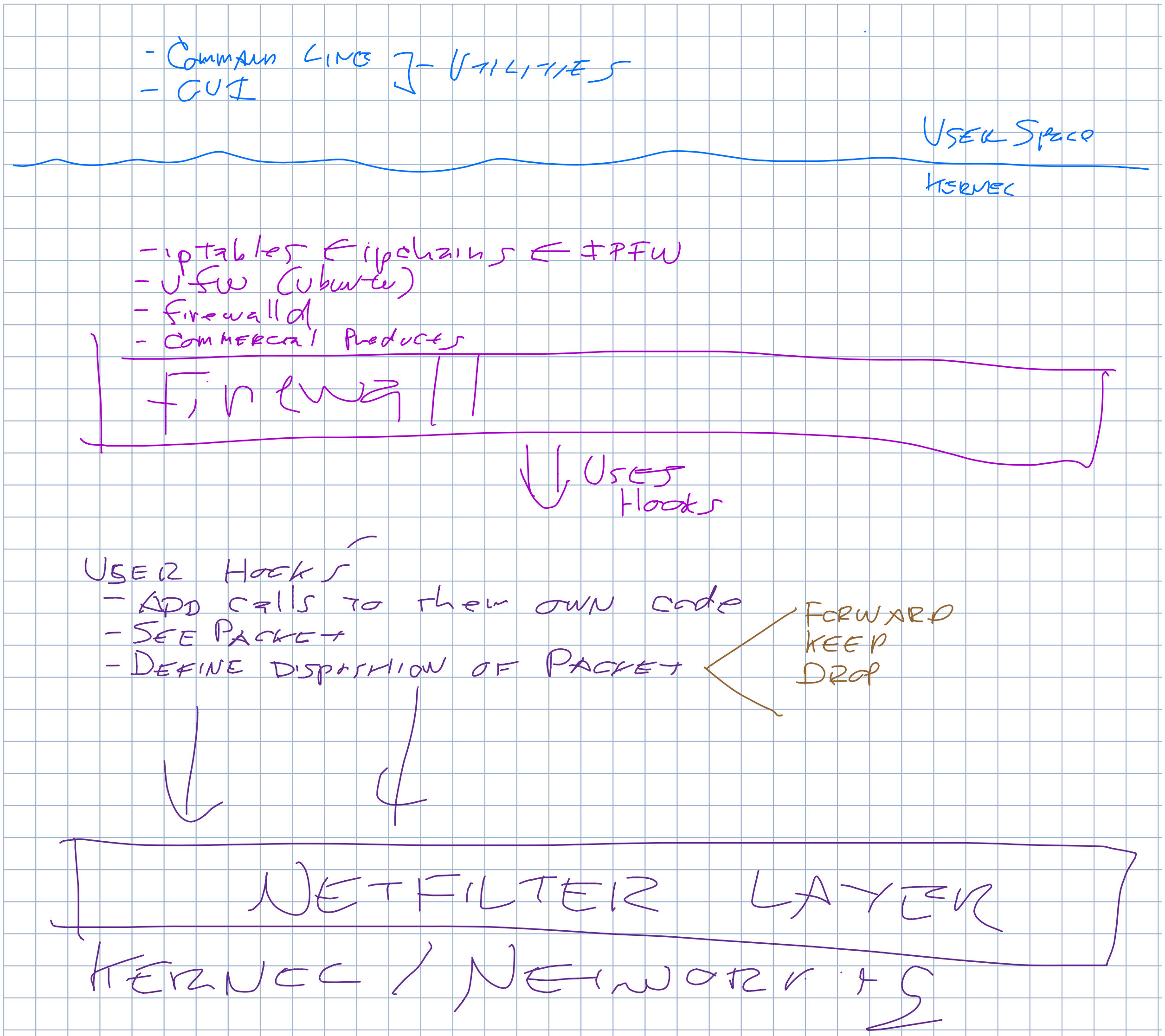
Kernel space

User space

Out

IN


PREROUTING
OUTPUT
eth0
./a.out
route?
No
Yes
eth1
INPUT
POSTROUTING
FORWARD



- Command Line
- GUI

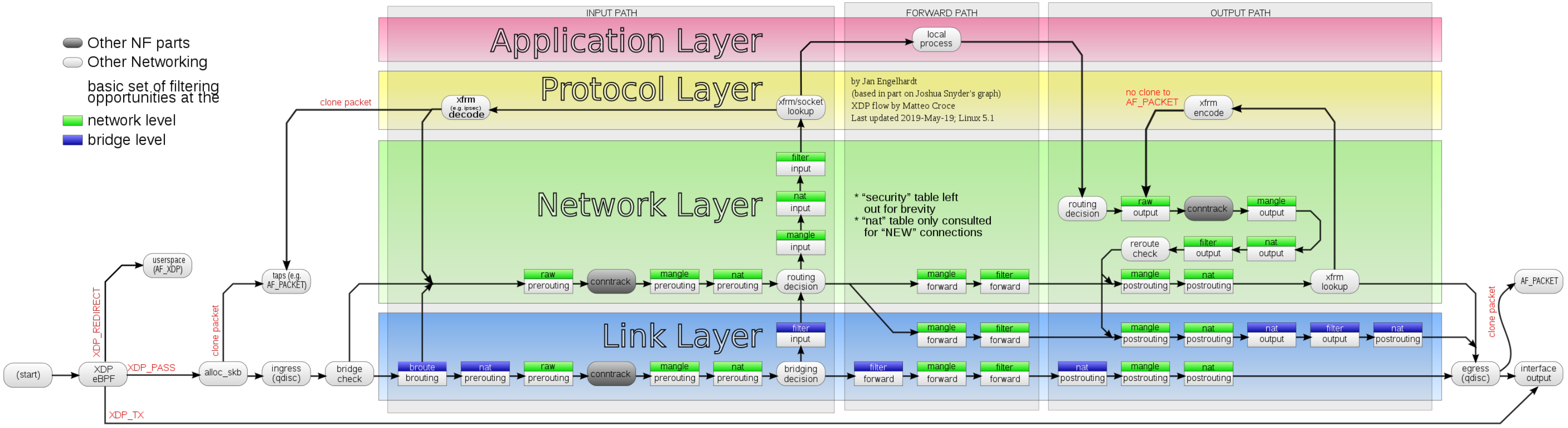
- iptables & ipchains & IPFW
- ufw (ubuntu)
- firewalld
- commercial products

User Hooks
- Add calls to their own code
- See Packet
- Define disposition of Packet

iptables Concepts

- Tables->Chains->Rules->Policies

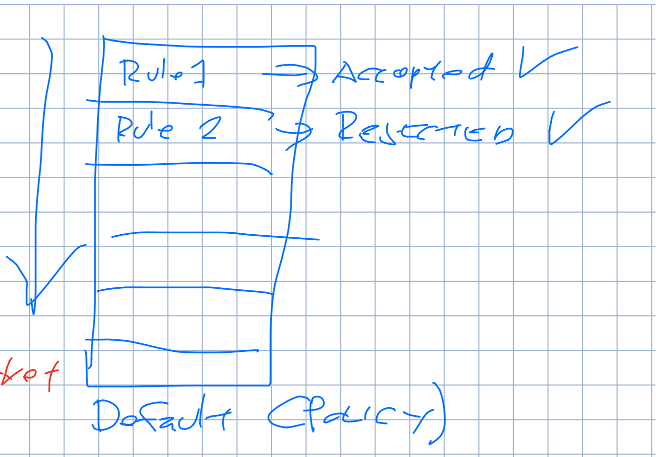
Packet flow in Netfilter and General Networking



by Jan Engelhardt
(based in part on Joshua Snyder's graph)
XDP flow by Matteo Croce
Last updated 2019-May-19; Linux 5.1

* "security" table left out for brevity
* "nat" table only consulted for "NEW" connections

SET OF RULES
↳ Grouped into a chain



RULES
- Match / Criteria
  ↳ Do I care about this packet
- TARGET
  ↳ What to do w/packet

```
iptables -t FILTER -A INPUT -s 123.45.67.89 -j DROP
iptables -t FILTER -P INPUT DROP
```

FILTER Table	NAT Table	MANGLE	RAW
CHAINS	Chains		Lower Level
- INPUT	- PREROUTING		-L2
- FORWARD	- POSTROUTING		
-OUTPUT	-OUTPUT		

CONNTRACK MODULE - CONNECTION TRACKING

<FW WAN I/P

192.168.1,4 → 170.41.41.4 / :3456

192.168.1.4 ← Table

Connection State

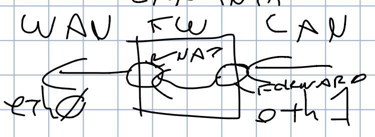
Implementing NAT

WAN ↓ intf

Type of NAT ← SNAT/DNAT

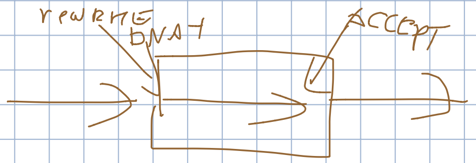
```
iptables -t NAT -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A FORWARD -i eth1 -j ACCEPT
```

↑ LAN intf

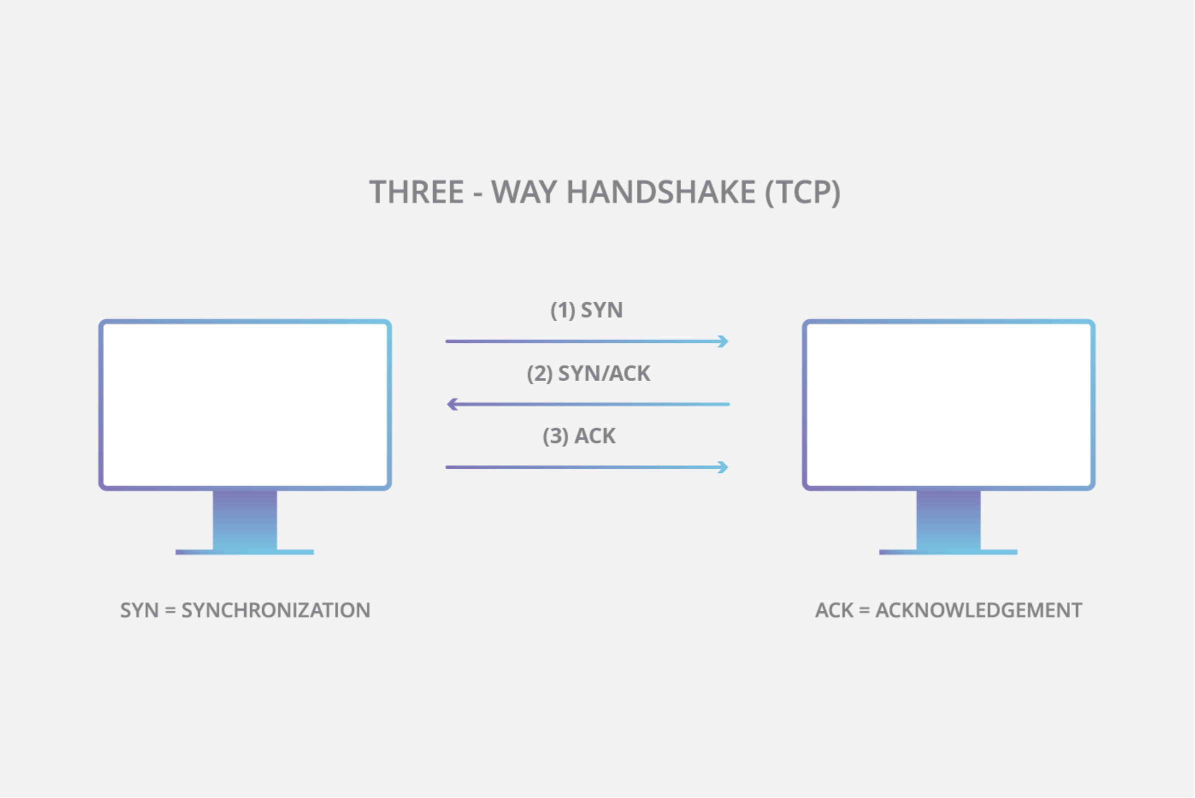


FORWARDING

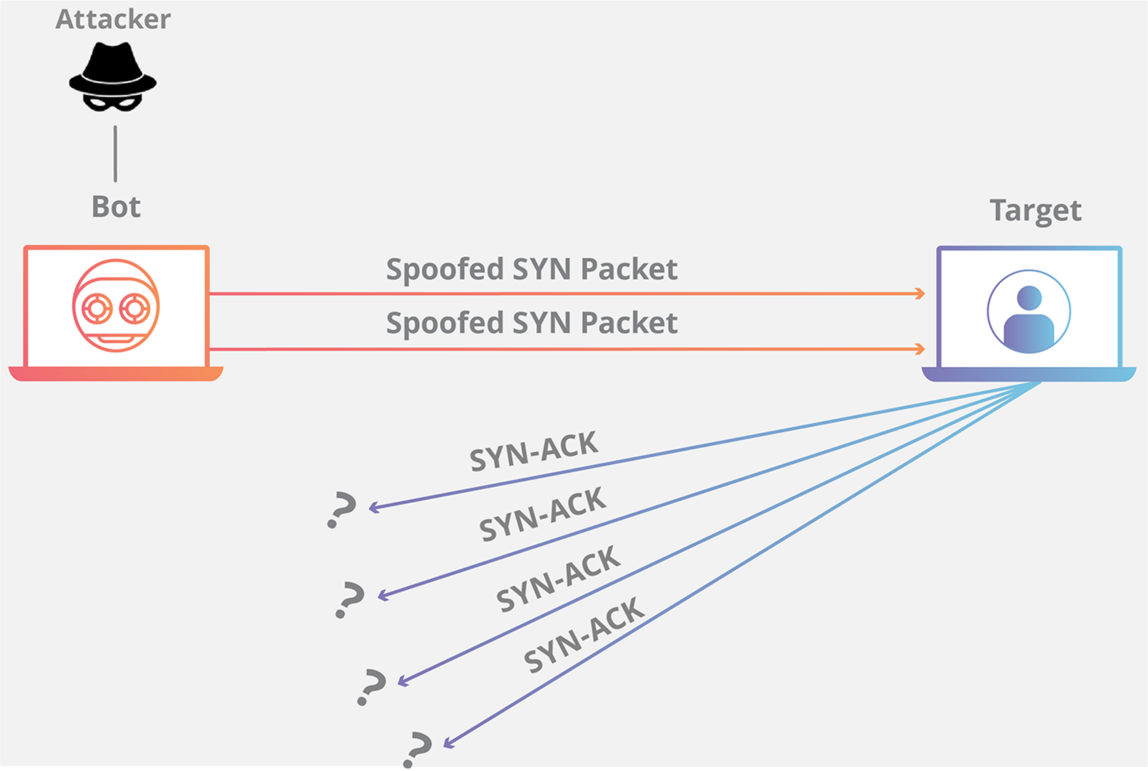
```
iptables -A PREROUTING -t NAT -i eth0 -p tcp -dport 80
         -j DNAT --to 192.168.1.2:8080

iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 8080
                                              -j ACCEPT
```



SYN Flood Attack



SYN Flood Attack



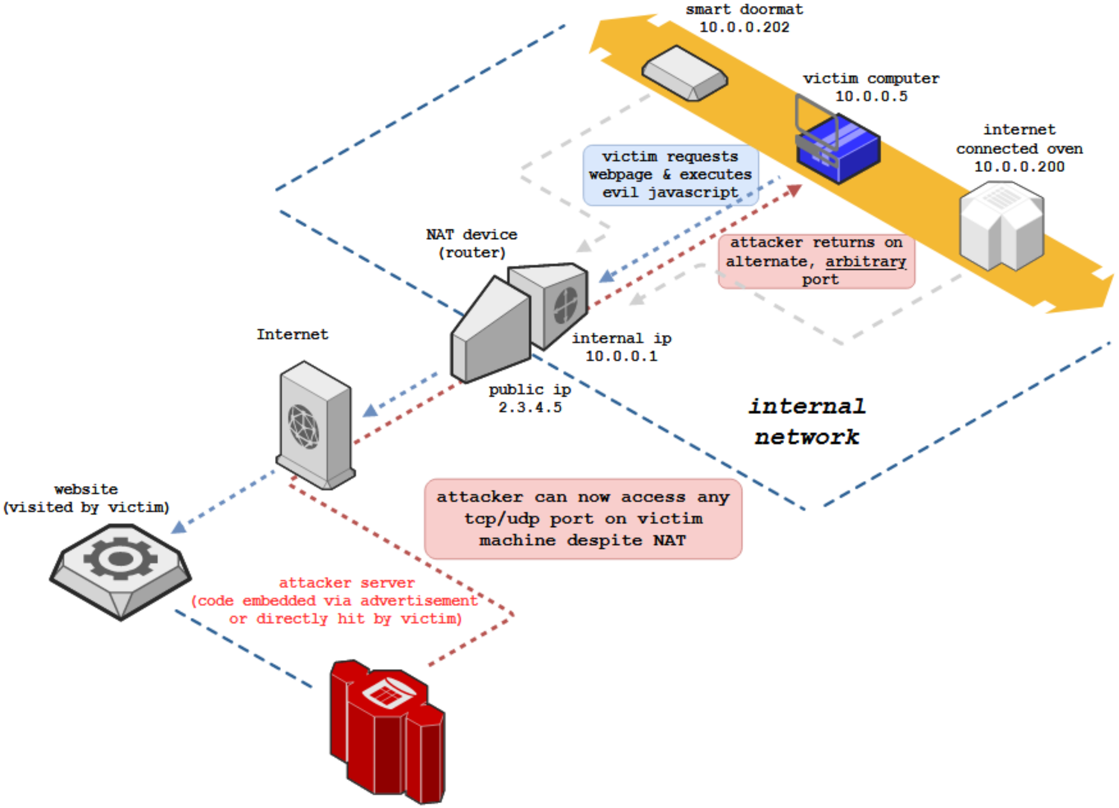
Fill SYN Table

- Denial of Service

SYN Flood Mitigations

- Limit on specific address
- REDUCE TIMEOUT
- LARGE SYN table
- Recycle oldest
- SYN COOKIES
  - NO SYN Table
  - SYN/ACK HAS INFO TO TRACK
- FRONT END
  - SMART TOOL
    - PATTERN OF ACTIVITY
  - CLOUDFLARE
    - SERVICE

NAT Slipstreaming


smart doormat
10.0.0.202
victim computer
10.0.0.5
internet connected oven
10.0.0.200
victim requests webpage & executes evil javascript
NAT device (router)
attacker returns on alternate, arbitrary port
internal ip
10.0.0.1
Internet
public ip
2.3.4.5
internal network
website (visited by victim)
attacker can now access any tcp/udp port on victim machine despite NAT
attacker server (code embedded via advertisement or directly hit by victim)