You like Networking?

Yes. You will love it.

Sign in :3

https://da.gd/KAVhb

whoami

Evan Deters

3rd Year CIS

ISSE

CCDC

Captain	2023-Present
Networking	2022-2023
Windows	2021-2022

CPTC

Moral Supporter	2021-Present

whoami

Marshall Ung | Shadowclaw

3rd Year CE

CCDC

- Alternate Threat Hunter 2022-2023
- Threat Hunter 2023

CPTC

- Alternate Team Member 2022
- Team Member 2023

Whoami

Dylan Tran

3rd Year CIS

Intern @ X-Force Red

CCDC

Linux Team 2021-2023

Linux Lead 2023-202?

CPTC

Team Member 2021-2023

Captain 2023-2024

Dylan Tran

@d_tranman

whoami

- jessica leung | @jeSSH
- CCDC business monkey
  - ex-windwos team
- co-head honcho @ SWIFT
- pentest @ Visa

Agenda

1 Intro to Networking

2 Competition Networking

3 Client Server Model

4 Firewalls!

5 OSI Model

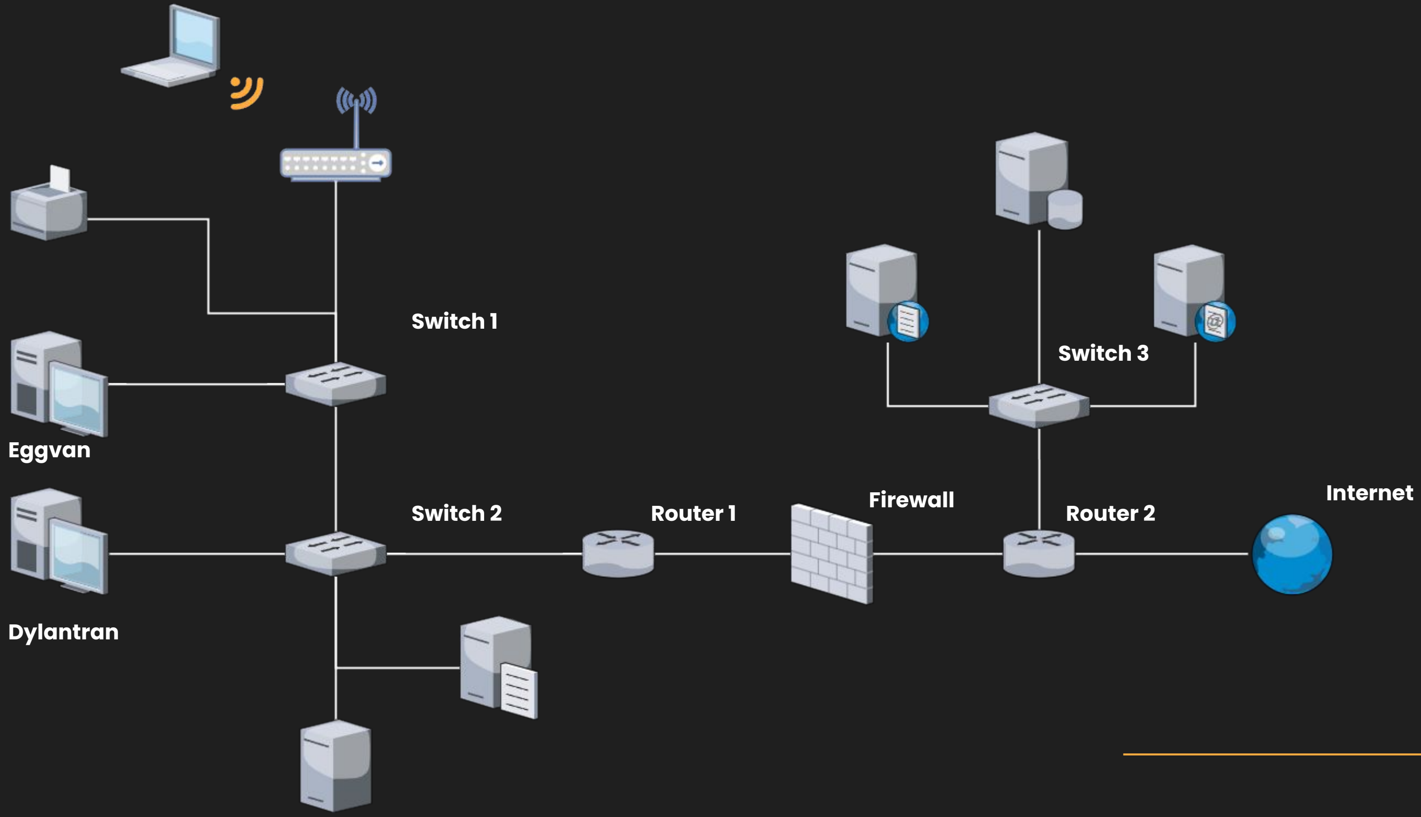
6 Lab

1

Intro to Networking

Alright then, let’s do some networking

Basic Topology



Network Devices

Anything on the network

- Computers, phones, routers, switches, etc.
- Contains at least one **Network Interface Card,** or **NIC**
  - Wired
  - Wireless

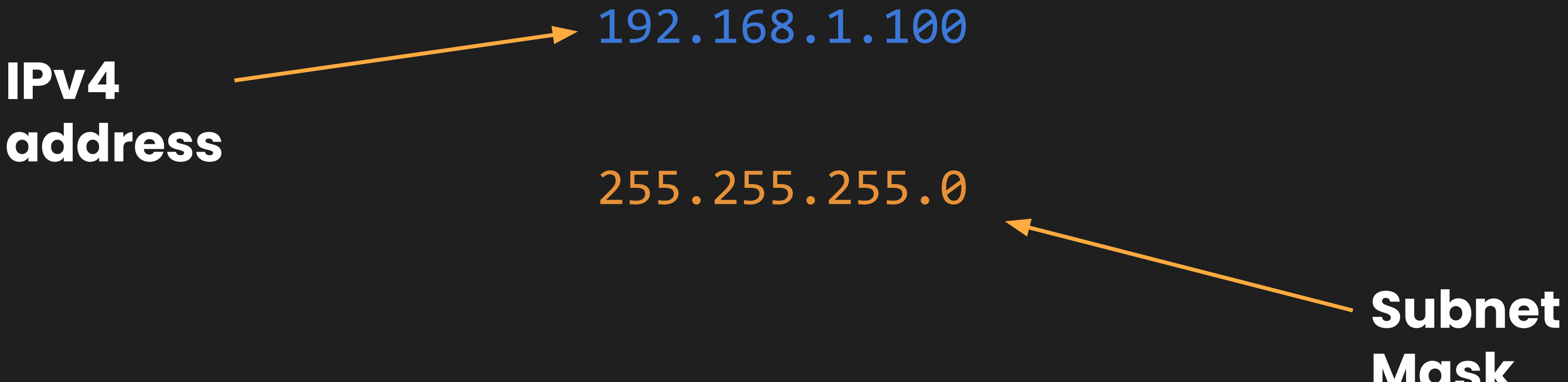
Lingo

- IP Address
- Subnet Mask
- Router
- Default Gateway
- Service

- Protocol
- Port
- Interface
- Firewall

SO THE ROUTER SAYS TO THE DOCTOR
IT HURTS WHEN IP.
Copyright 1997 Jeffrey Jeffords
quickmeme.com

Subnet Masks

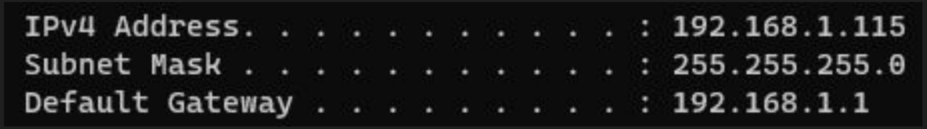


IPv4 address

192.168.1.100

255.255.255.0

Subnet Mask



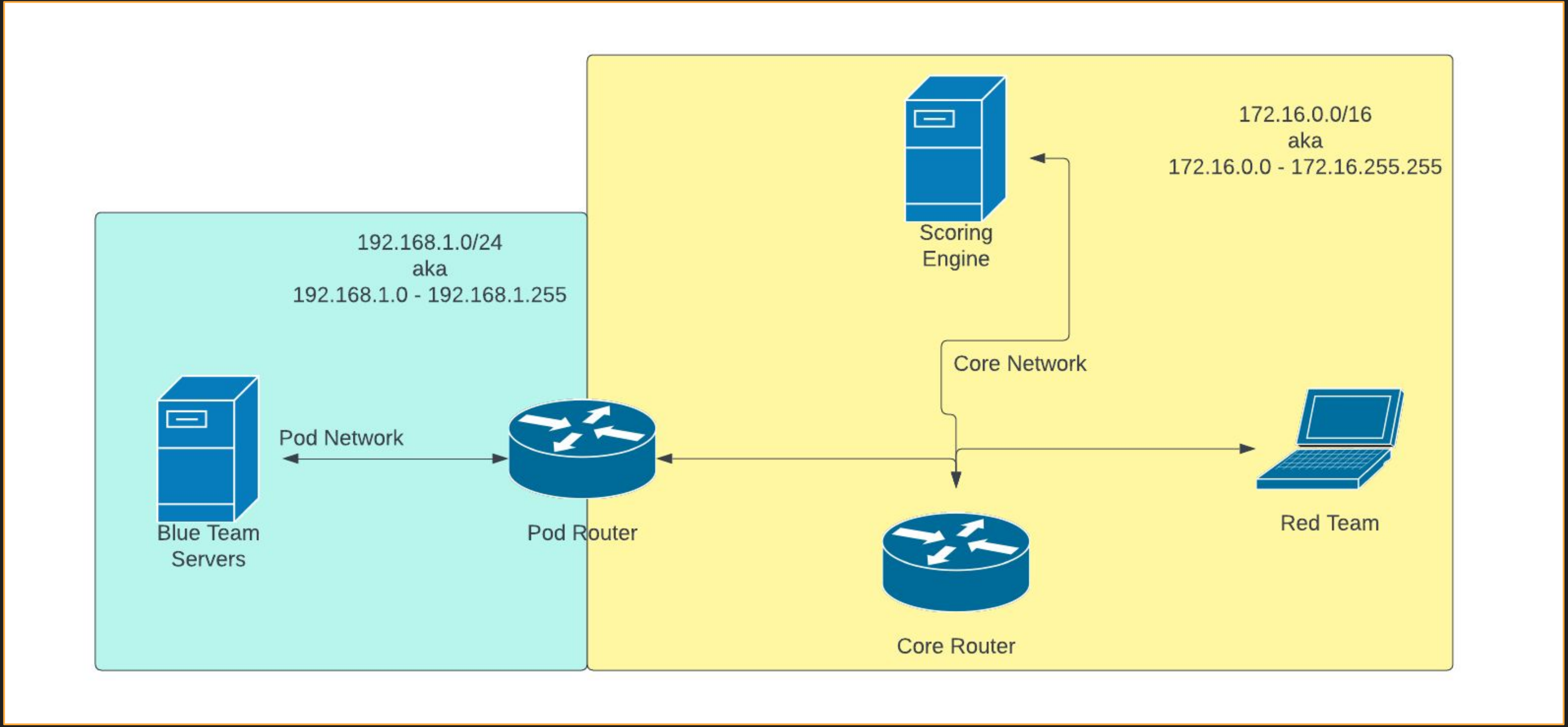
```
IPv4 Address. . . . . . . . . . . : 192.168.1.115
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

2

Competition Networking

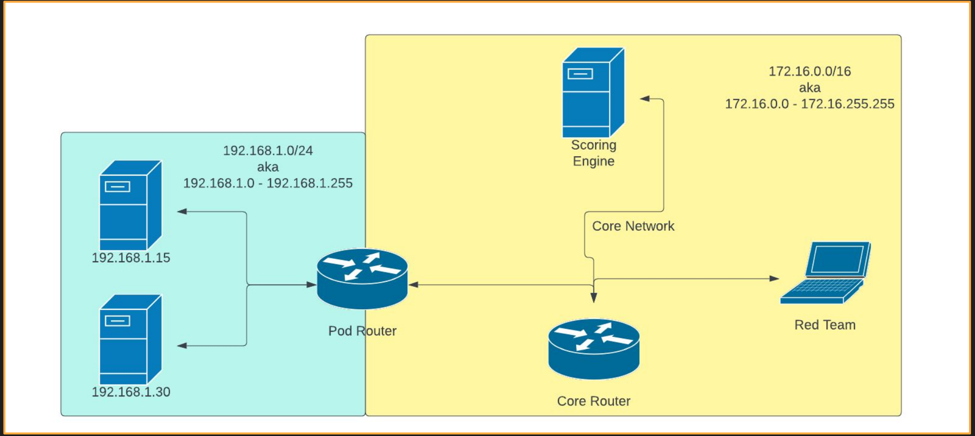
Networking Makes the Services go Round

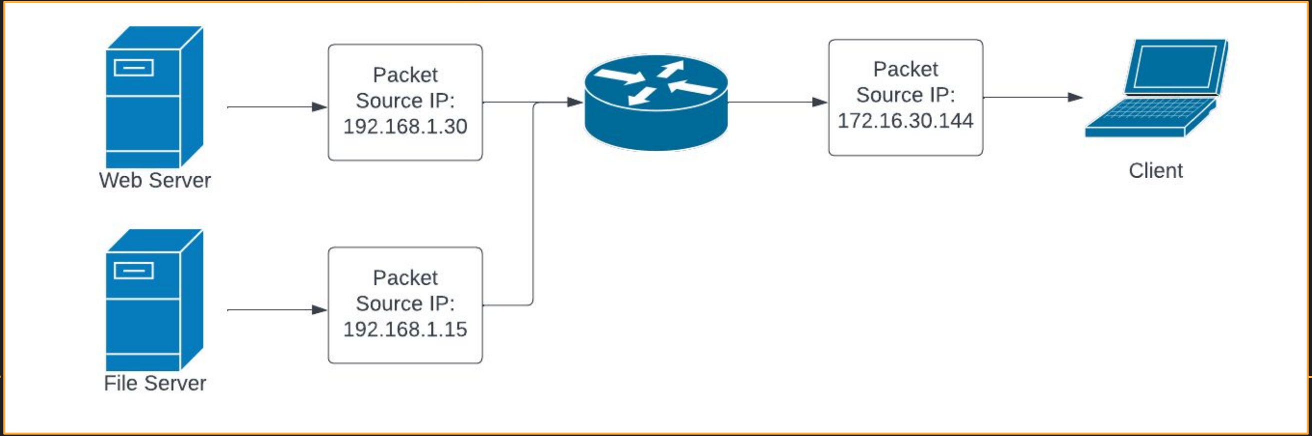
Competition Topology



NAT

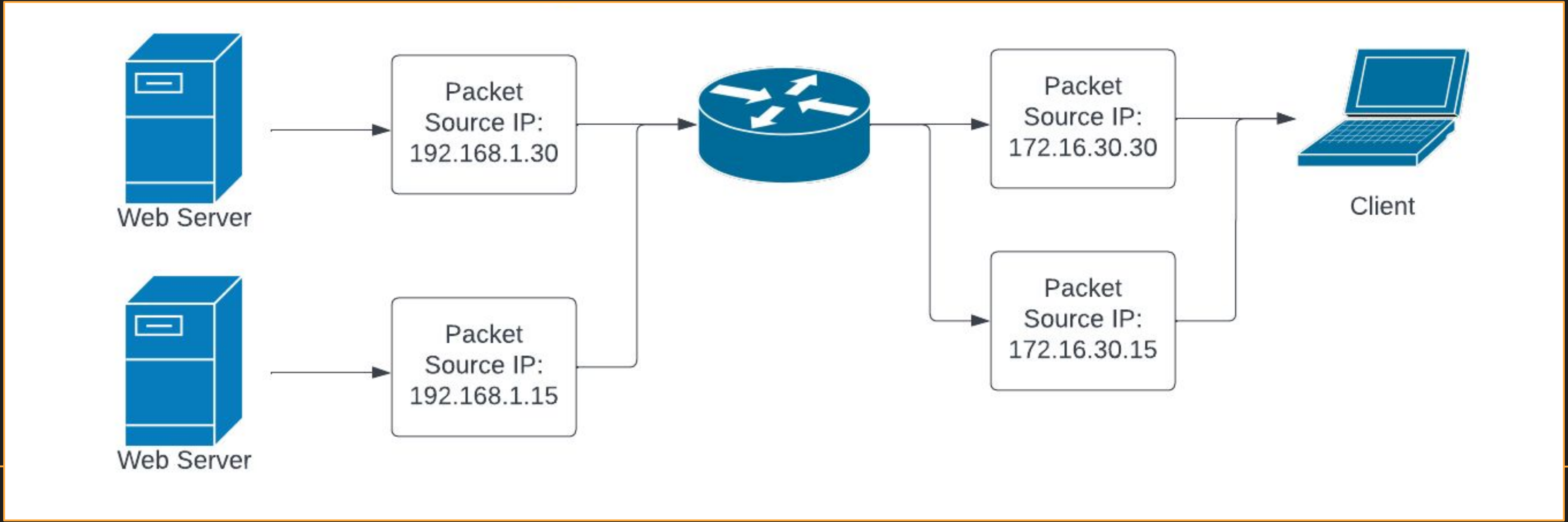
- Network Address Translation
- Built to conserve IP addresses
    - One-to-Many Translation




Web Server
Packet Source IP: 192.168.1.30
File Server
Packet Source IP: 192.168.1.15
Packet Source IP: 172.16.30.144
Client

1:1 NAT

- Direct Translations
- 192.168.1.0/24 → 172.16.30.0/24

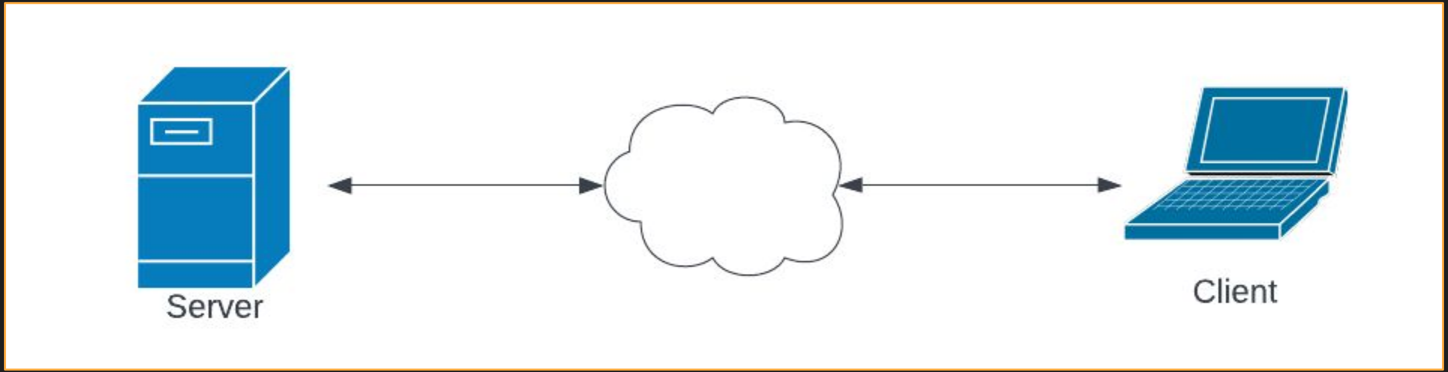


3

Client-Server Model

A Restaurant, but for Packets

Client-Server Model



What are ports?

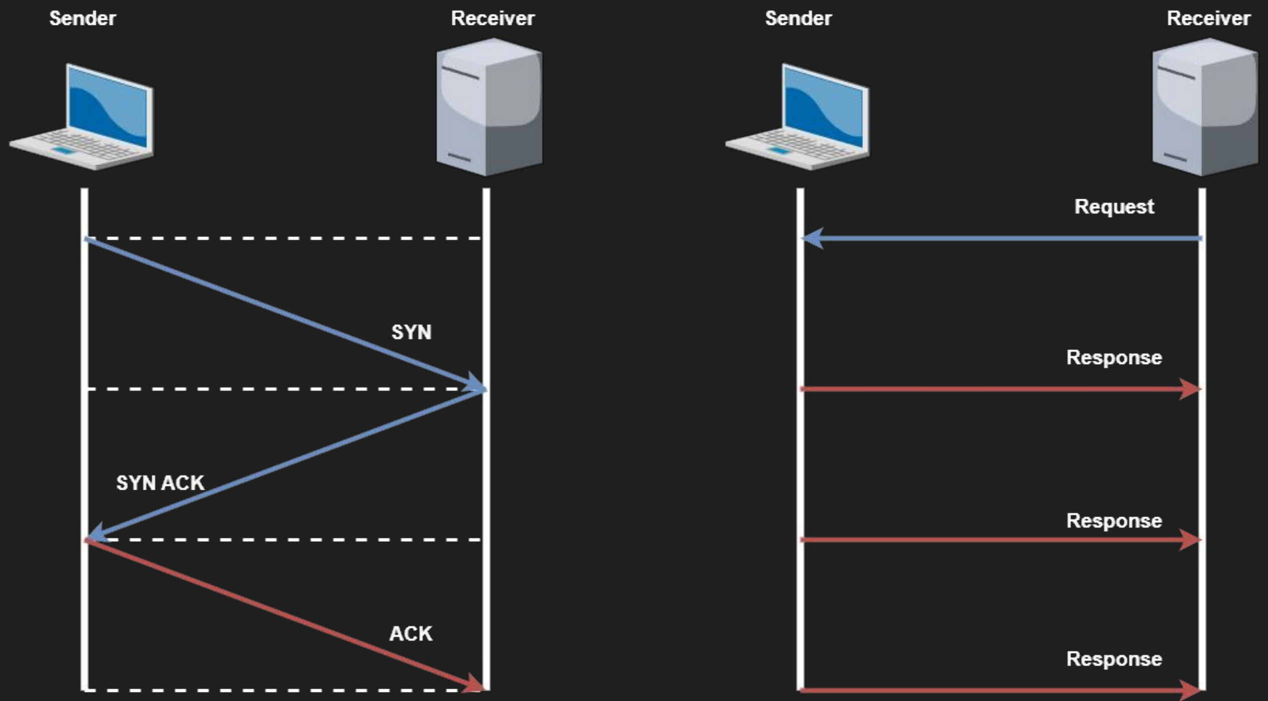
Numbers that identify specific running services on a machine

- Common port numbers
  - TCP 20 and 21 - FTP
  - TCP 22 - SSH
  - TCP 25 - SMTP
  - UDP 53 - DNS
  - TCP 80 - HTTP
  - TCP 443 - HTTPS
  - etc.

TCP and UDP

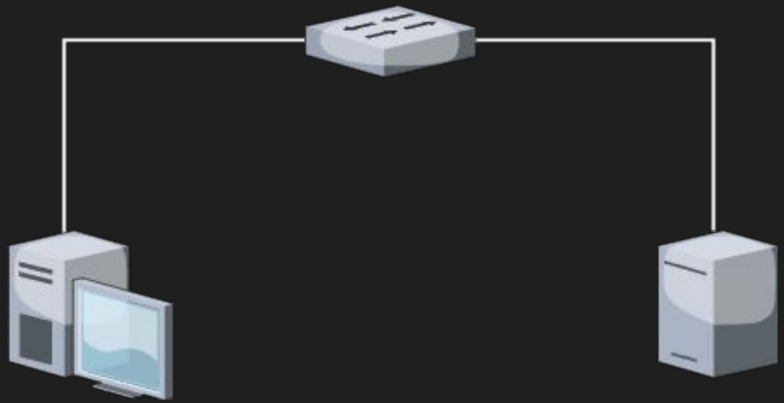
- TCP - Slow but reliable
  - Synchronization
  - Flow control
  - TCP Handshake
- UDP - Fast but unreliable
  - No error-checking
  - No acknowledgements
  - Just send data

TCP and UDP


Sender
Receiver
SYN
SYN ACK
ACK
Sender
Receiver
Request
Response
Response
Response

What are sockets?

Each end of a connection, basically a pairing between an IP and a port.



IP: 192.168.1.10
MAC: AA:AA:AA:AA:AA:AA

IP: 192.168.1.58
MAC: EE:EE:EE:EE:EE:EE

192.168.1.10:57138 → **192.168.1.58:80**

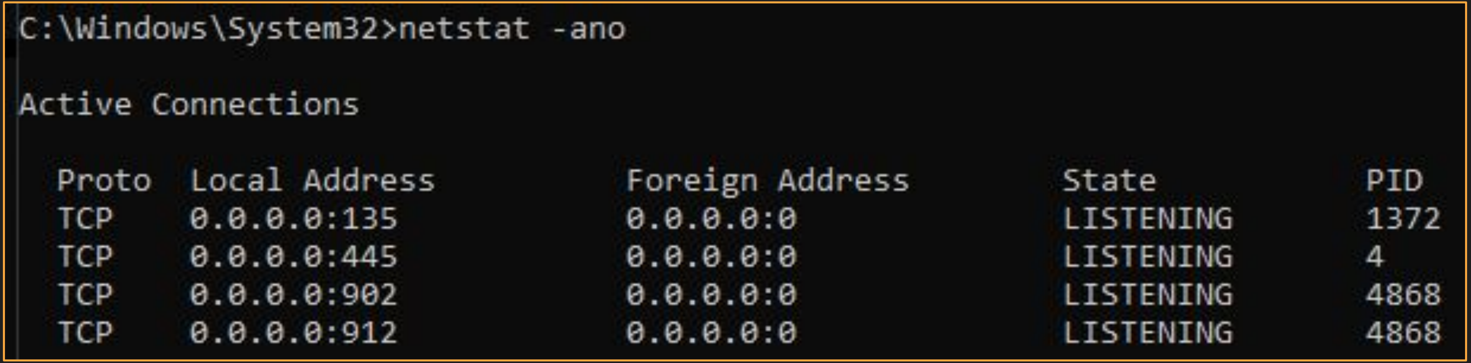
why

Identify normal/abnormal traffic

- Is it coming from scoring engine/orange team? Or is it red team?

Troubleshooting services

- Firewall issue? Service disabled?



```
C:\Windows\System32>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1372
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4868
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4868
```

Ports & Services Review

- TCP and UDP
- Ports - numbers that identify a running service/application
- Common ports
- Source and destination addresses/ports
  - **Ephemeral ports** on client-side
  - Sockets

4

Firewalls

FIREWALL TIME BABEYY

Block IPs

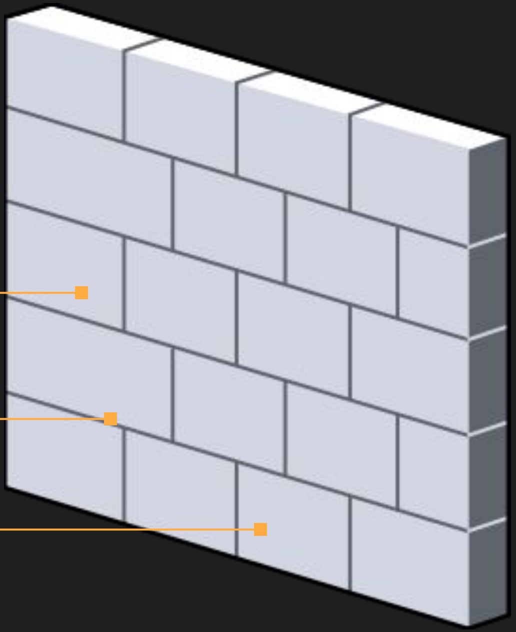
Can block a whole
subnet or individual.

Block Ports

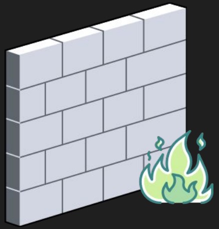
Block which ports the
external network can
access on the LAN

Filtering

Ingress and Egress
filtering rules.



NGFW vs Traditional

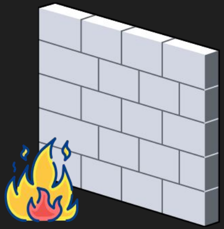


NGFW

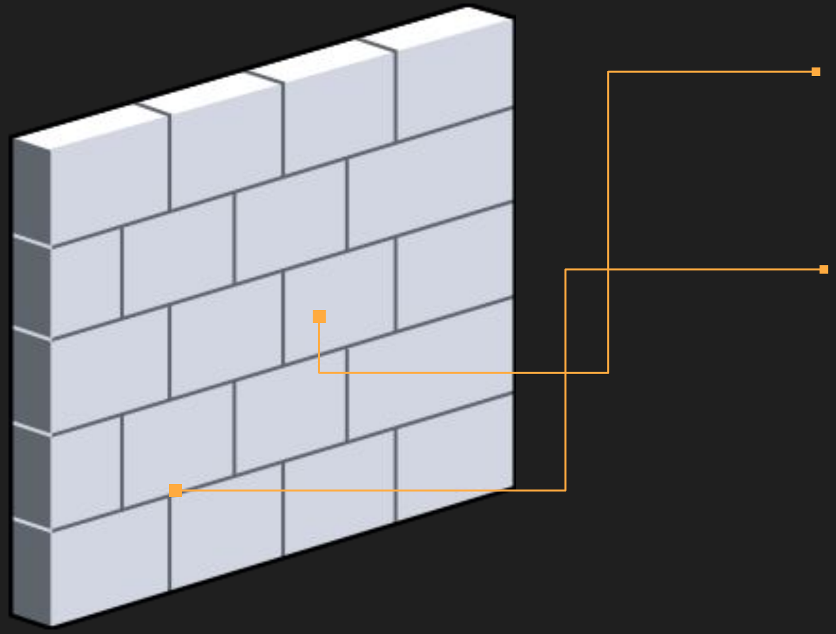
- Stateful Inspection on incoming and outgoing traffic
- Comprehensive application control and visibility
- Easy to install, configure, integrate security tools, reducing administrative controls
- SSL traffic can be decrypted and inspected.
- IPS & IDS are integrated

Traditional

- Stateful Inspection on incoming and outgoing traffic
- Partial application control and visibility only
- Managing security tools separately is $$$
- Cannot decrypt and inspect SSL traffic
- Integrated IPS and IDS are deployed separately in traditional firewalls



Stateless vs Stateful



Stateless

ACL. Looks at
Individual packets.

Stateful

Traffic patterns and flows.
Remembers connections.

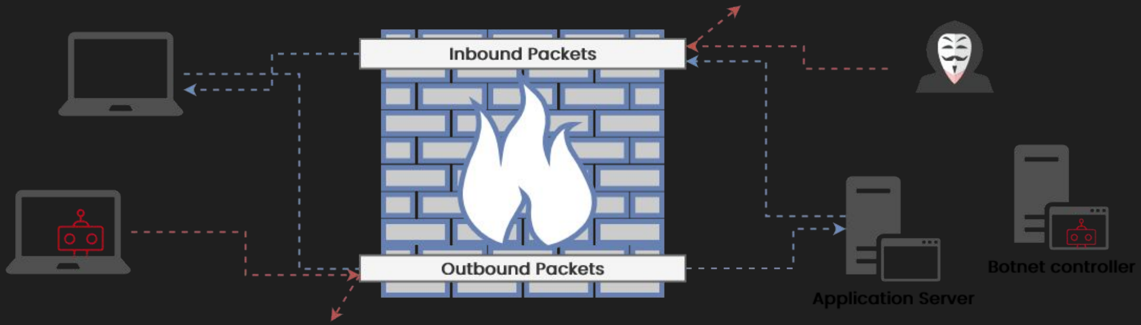
FW Example

Inbound

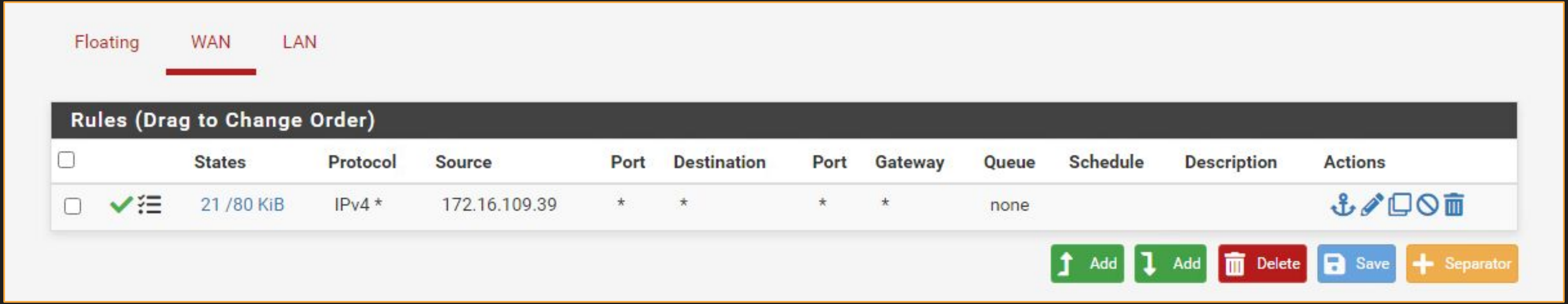
- Only allow required services
- Allow certain subnets
- Allow certain ip addresses

Outbound

- Block everything going outbound (break internet)



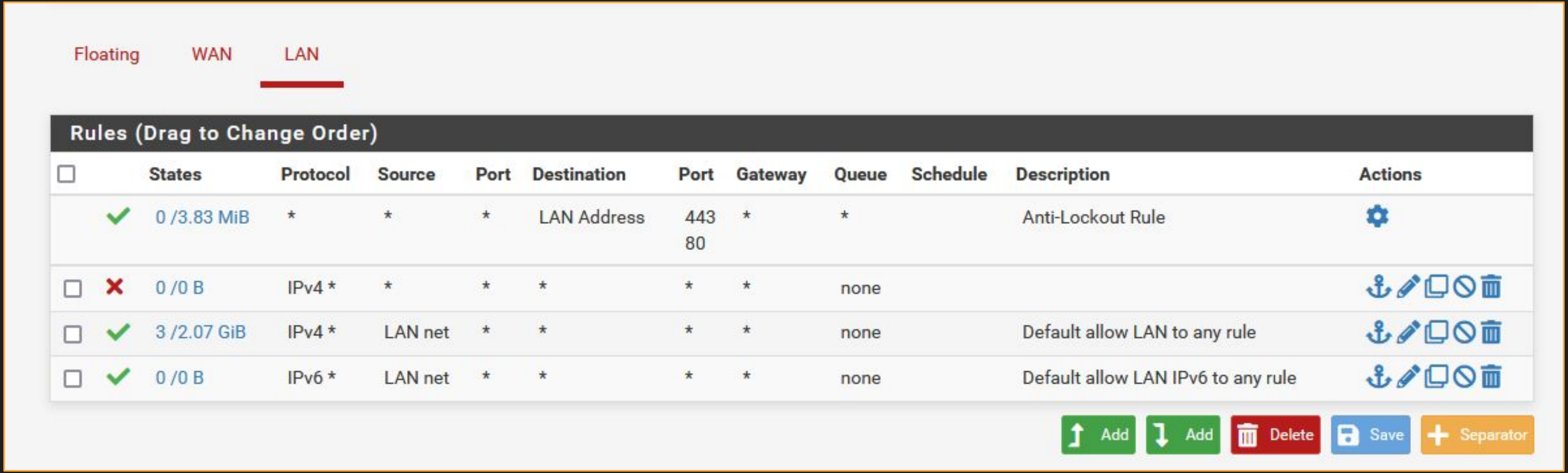
WAN Firewall



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	21 /80 KiB	IPv4 *	172.16.109.39	*	*	*	*	none			

LAN Firewall



Rules (Drag to Change Order)

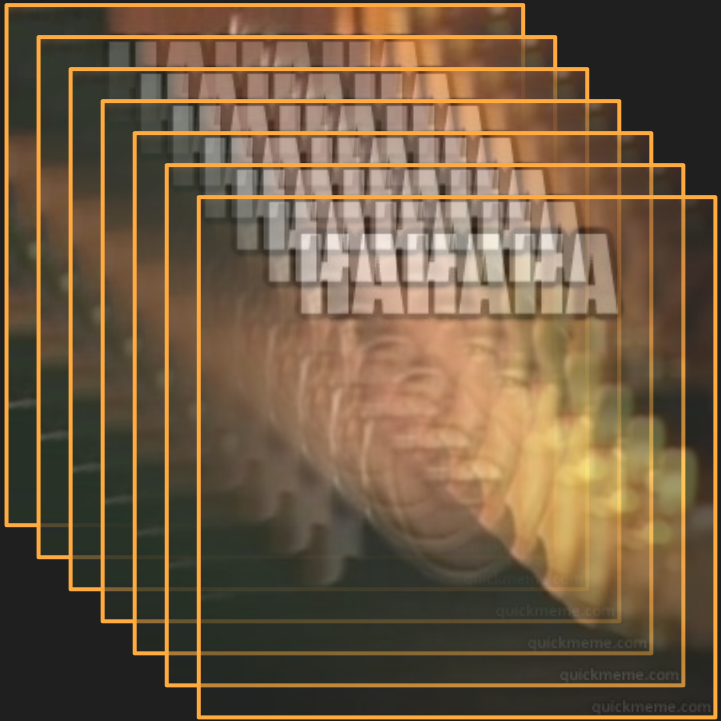
☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /3.83 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
☐	✗	0 /0 B	IPv4 *	*	*	*	*	*	none			⚓ ✎ ⧉ ⊘ 🗑
☐	✓	3 /2.07 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑
☐	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ⧉ ⊘ 🗑

Firewall Demo

5

OSI Model

no



6

Lab

Thanks!

Any questions? Questions are very cool. Please ask questions I am very lonely :((