You will love networking.

Yes. You will.

whoami

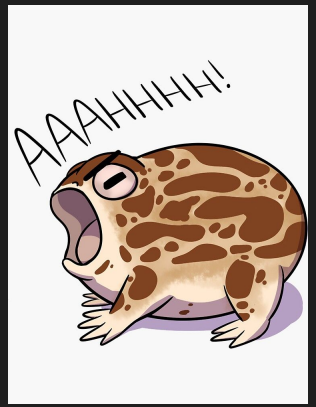
Natalie Tran | @natworking

Sysadmin Intern @ Genentech

CCDC Captain 2025-2026
CCDC Networking 2024-2025

SWIFT VP 2025-2026
SWIFT Alumni Coordinator 2024-2025

i like frogs :D



Agenda

1. Intro to Networking
2. Competition Networking
3. Client Server Model
4. Firewalls!
5. Lab

1

Intro to Networking

Not the LinkedIn one

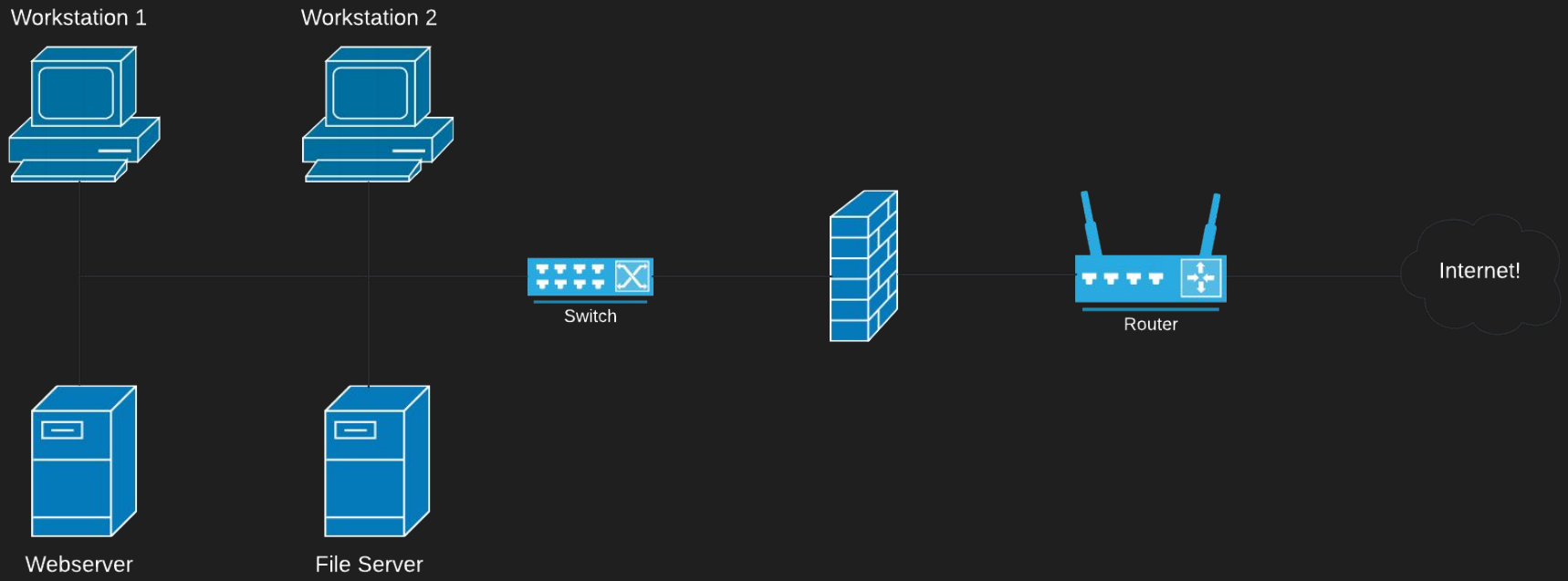
Network

System of interconnected network devices
- Communicate and share resources

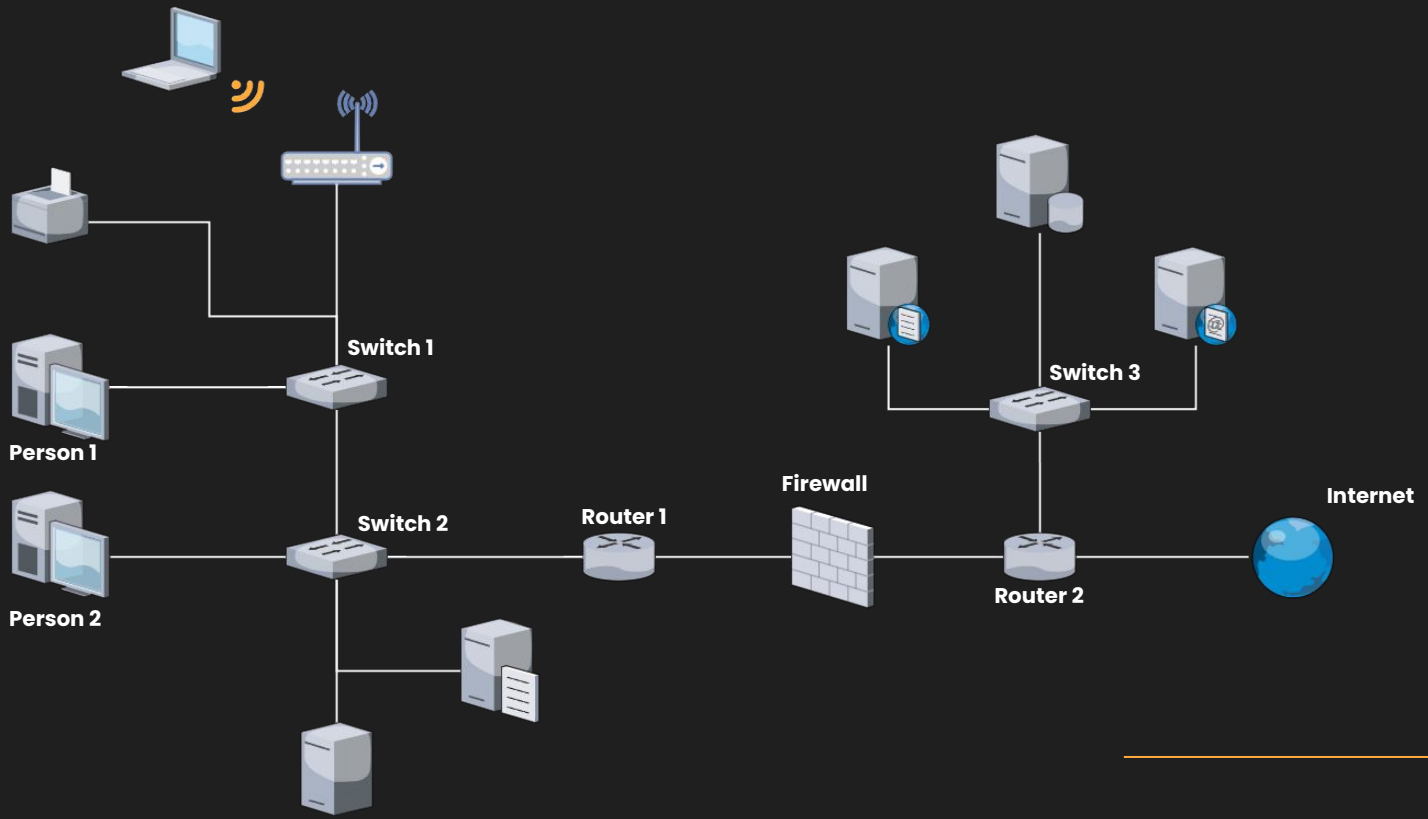
Network Devices

Anything on the network
- Computers, phones, routers, switches, etc.
- Contains at least one **Network Interface Card** (NIC)
  - Wired or wireless connection to internet

Basic Topology



Basic Topology?



Lingo

- IP Address
- Subnet Mask
- Router
- Default Gateway
- Service
- Protocol
- Port
- Interface
- Firewall

Subnet Masks

IPv4 address → 192.168.1.100

255.255.255.0 → Subnet Mask

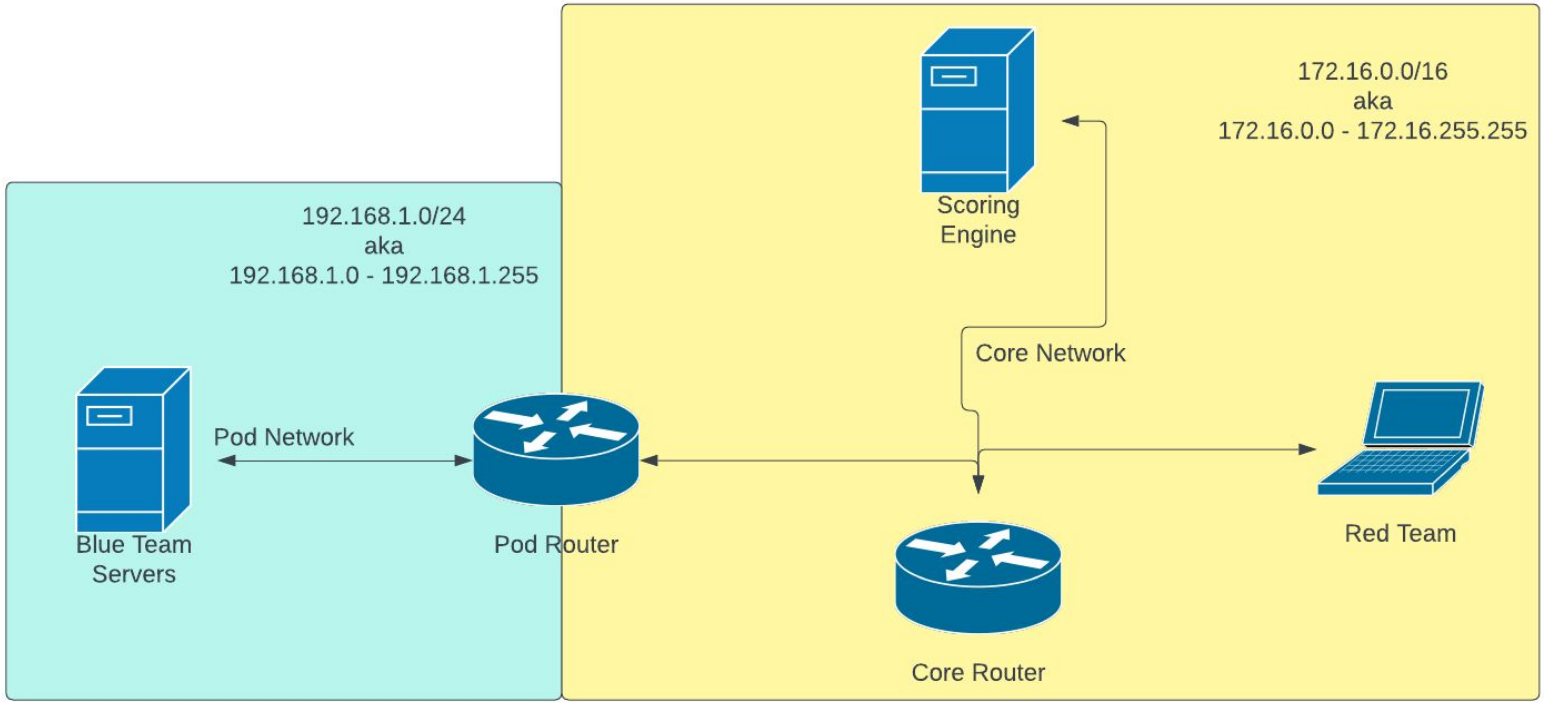
```
IPv4 Address. . . . . . . . . . . : 192.168.1.115
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

2

Competition Networking

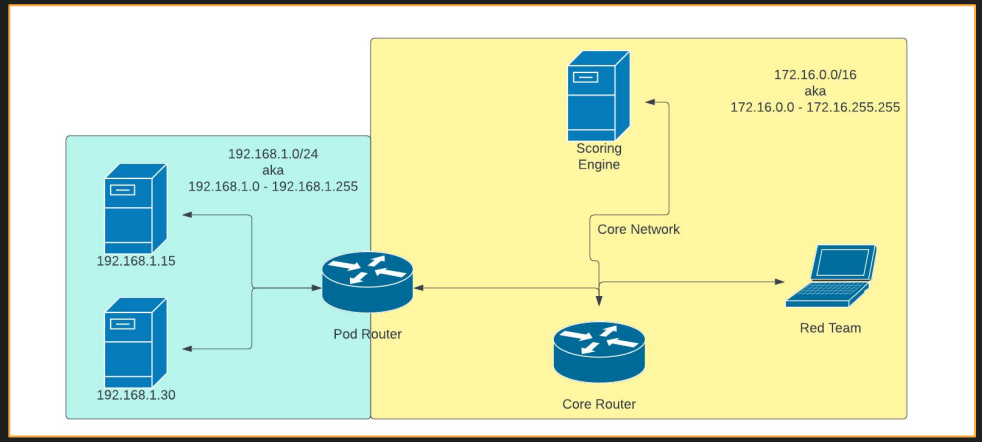
Services go brrrrr

Competition Topology

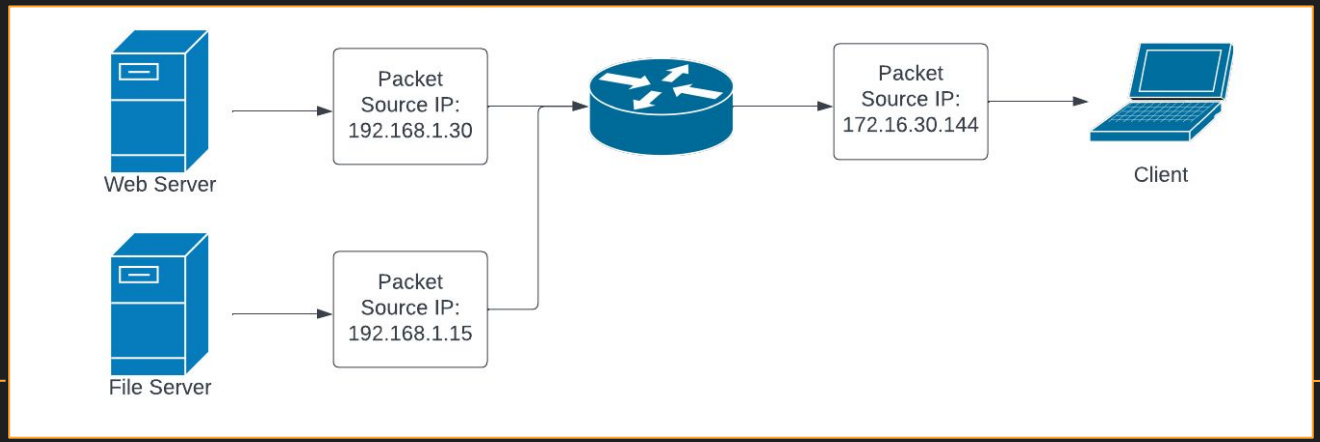


NAT

- Network Address Translation
- Built to conserve IP addresses

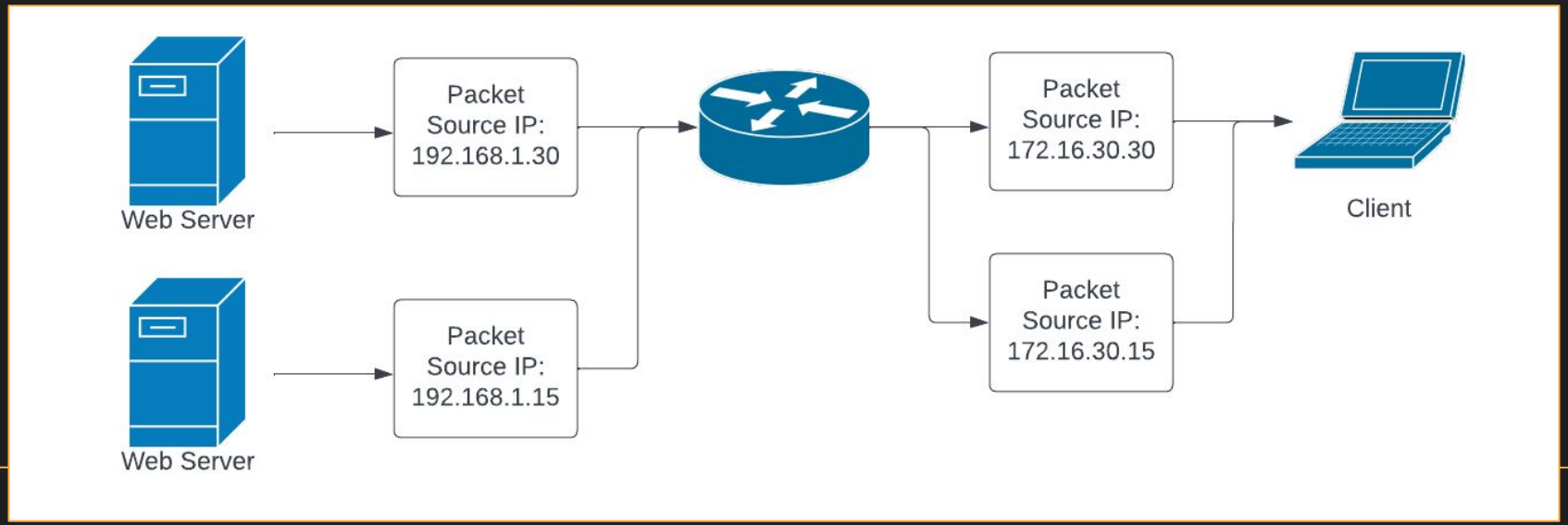


One-to-Many Translation:



1:1 NAT

- Direct Translations
- 192.168.1.0/24 → 172.16.30.0/24

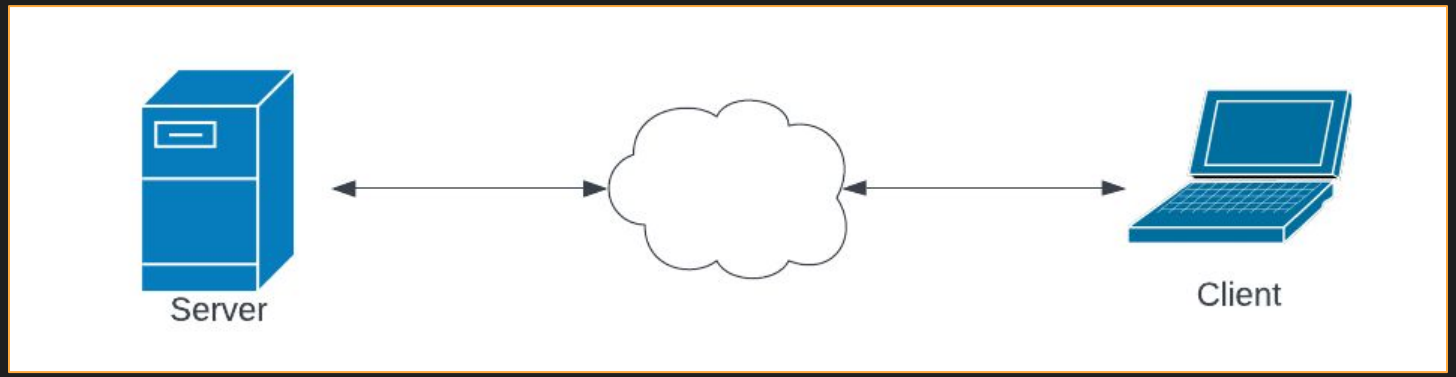


3

Client-Server Model

Packet restaurant

Client–Server Model



What are ports?

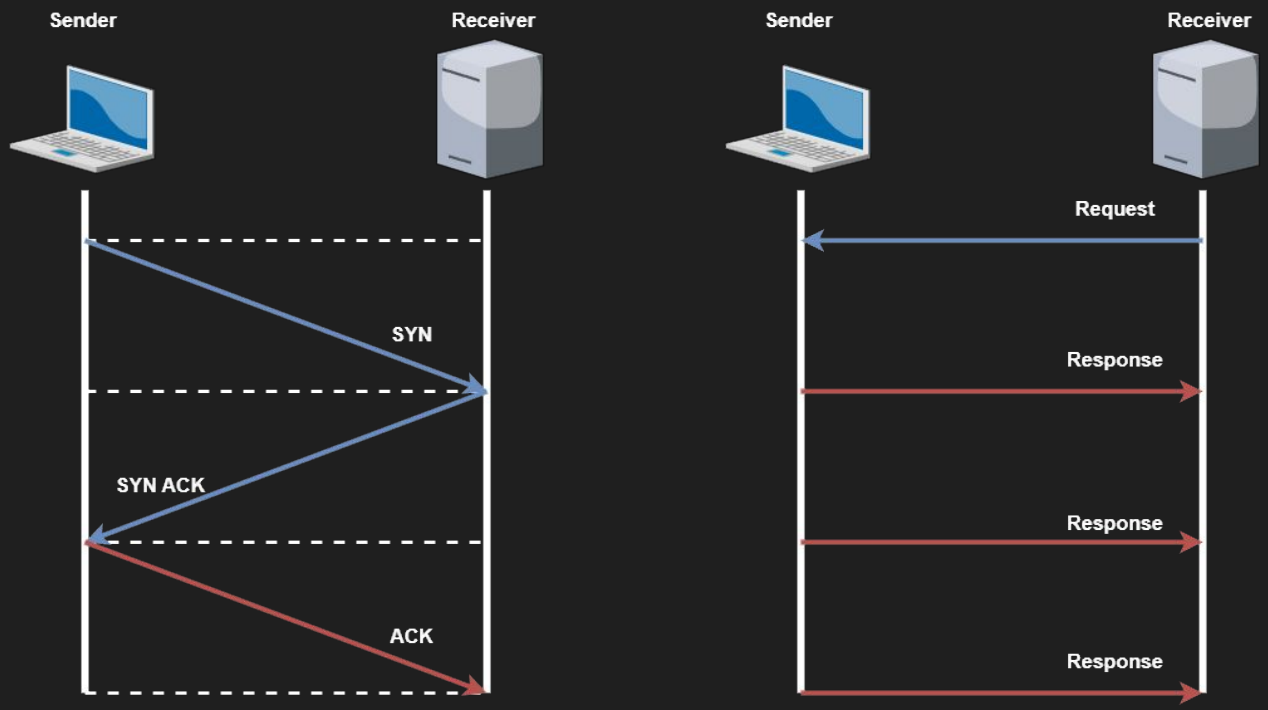
Numbers that identify, along with an IP address, which network socket to connect to on a given device.

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

TCP and UDP

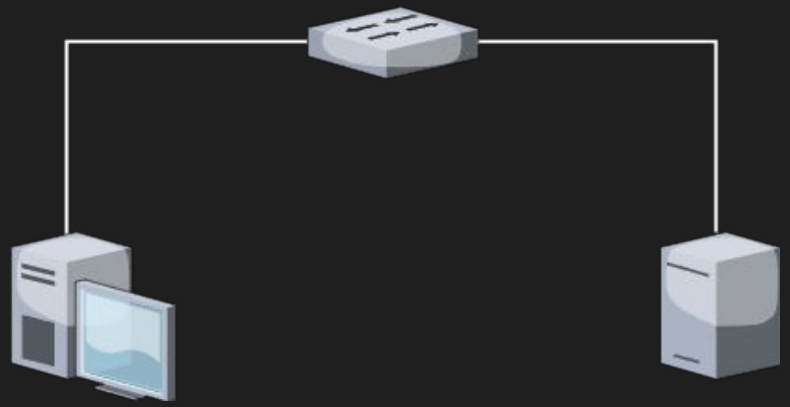
- TCP - Slow but reliable
  - Synchronization
  - Flow control
  - TCP Handshake
- UDP - Fast but unreliable
  - No error-checking
  - No acknowledgements
  - Just send data

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 is this important?

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
- Source and destination addresses/ports
  - **Ephemeral ports** on client-side
  - Sockets

4

Firewalls

Not a waterwall.

Block IPs

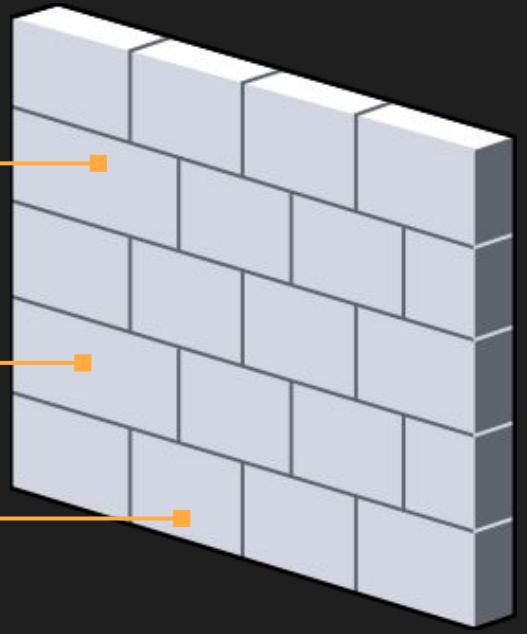
Can block a whole subnet or individual.

Block Ports

Block which ports the external network can access on the LAN

Filtering

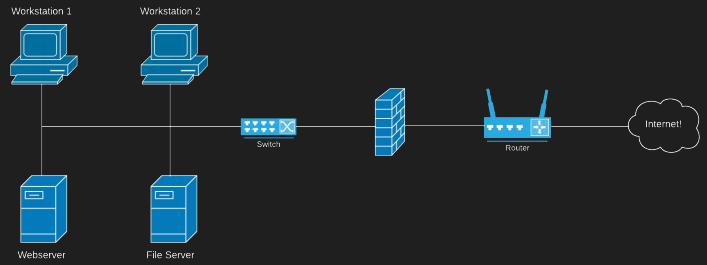
Ingress and Egress filtering rules.



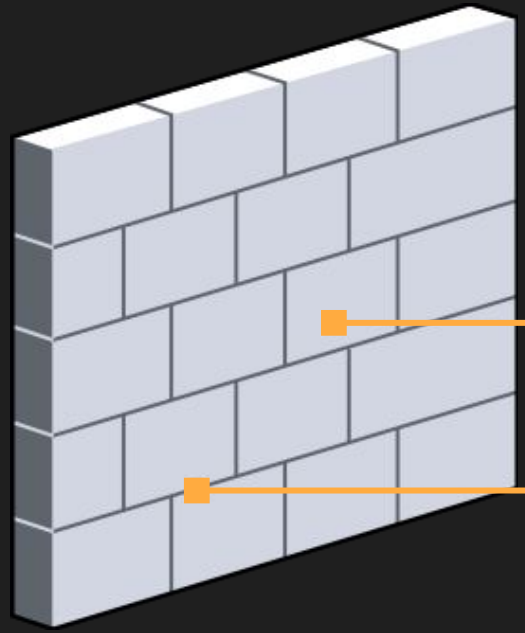
Host Firewall vs Network Firewall

- Host-based firewall
- Filters inbound and outbound traffic for a single device
- Two different rulesets
- Ex. a Windows file server has a Windows Firewall

- Network-based firewall
- Filters inbound and outbound traffic for LAN and WAN
- Four different rulesets
- Ex. a network has a Cisco Firepower Firewall



Stateless vs Stateful



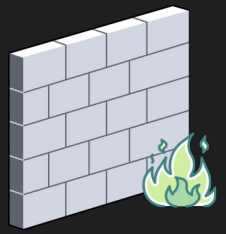
Stateless

ACL. Looks at
Individual packets.

Stateful

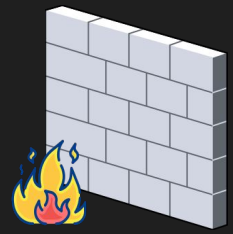
Traffic patterns and flows.
Remembers connections.

NGFW vs Traditional



- 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

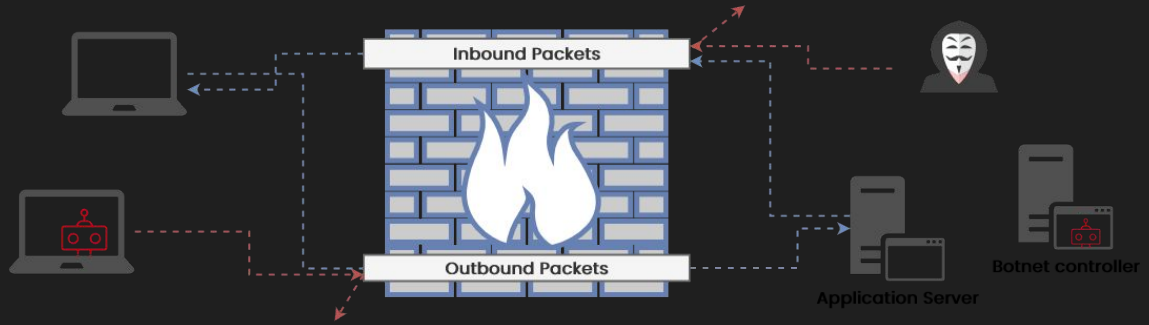
- Stateful Inspection on incoming and outgoing traffic
- Partial application control and visibility only
- Managing security tools separately is $$$
- Cannot decrypt and inspect SSL traffic
- Integrated IPS and IDS are deployed separately in traditional firewalls



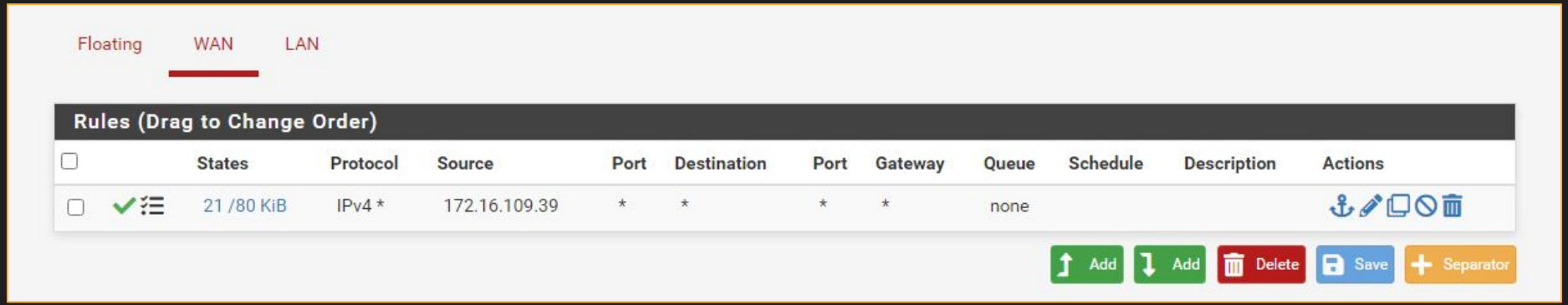
FW Example

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

Outbound
- Block everything going outbound (break internet)



WAN Firewall



LAN Firewall

Floating WAN LAN

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	

Add Add Delete Save Separator

6

Lab !!

(it's not packet tracer, i swear)

Homework

https://jessh.zip/2025ccdchw-3

Thanks!

Any questions? Please ask questions; we are available to help :D