Firewalls

UBNetDef, Spring 2024
Week 3

Lead Presenter:
Ethan Viapiano

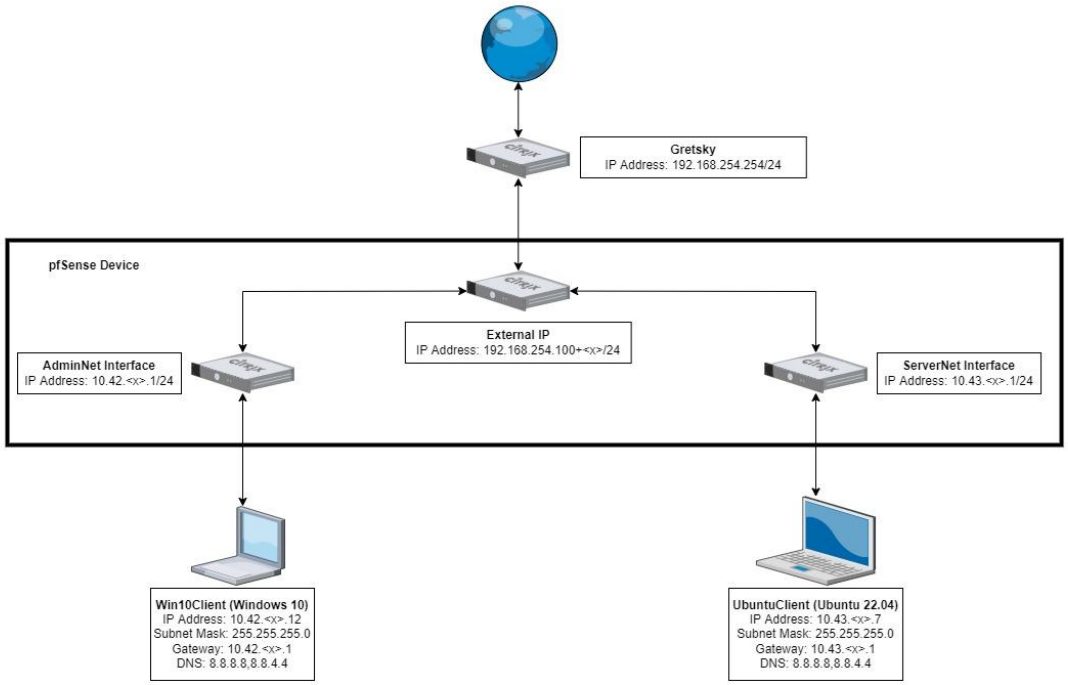
Learning Objectives

- More networking
- Specifics of transport layer of OSI Model
- TCP Handshake
- Understanding of directional flow
- Understanding of the various types of firewalls
- Able to understand firewall rules and configure them yourself

Agenda – Week 3

- Networking
  - Current Network State
  - Networking Part 2: Ports and Packets
  - In class exercise: TCP Packet Polo
- Migration Activity
- Firewalls
  - Types of Firewalls
  - In class exercise: TCP Packet Polo (with a firewall)
  - In class exercise: Login to pfSense
- Firewall and Packet Headers
- The Logic of Firewalls
  - How Traffic Flows
  - Default Rules
- pfSense Activity
- Homework Prep
- Summary/Wrap Up

Current Network State



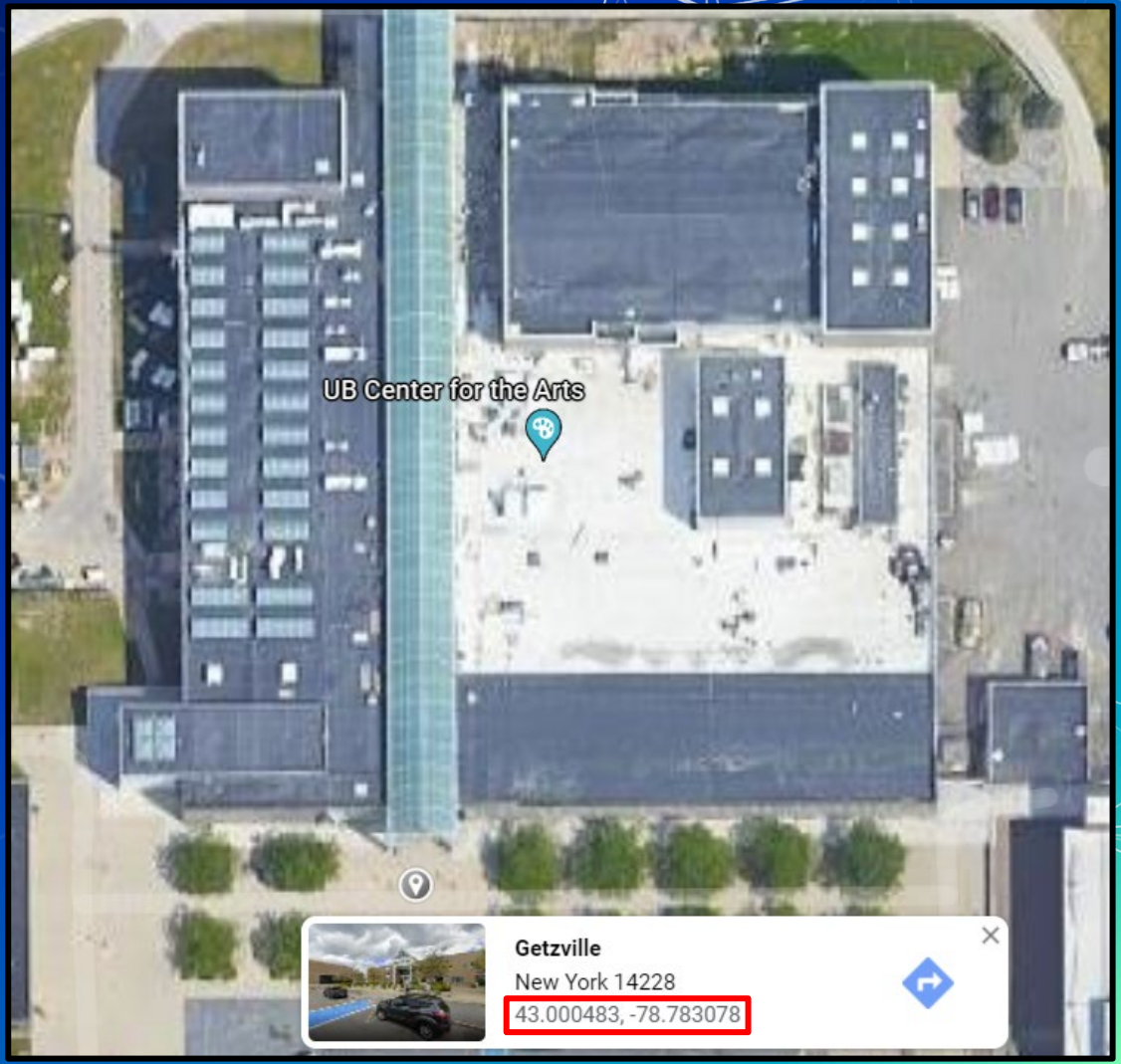
Intro to the Transport Layer

Transport Layer

- Data is transmitted using network packets
- Packets contain headers
  - Headers tell networking appliances what to do with packets

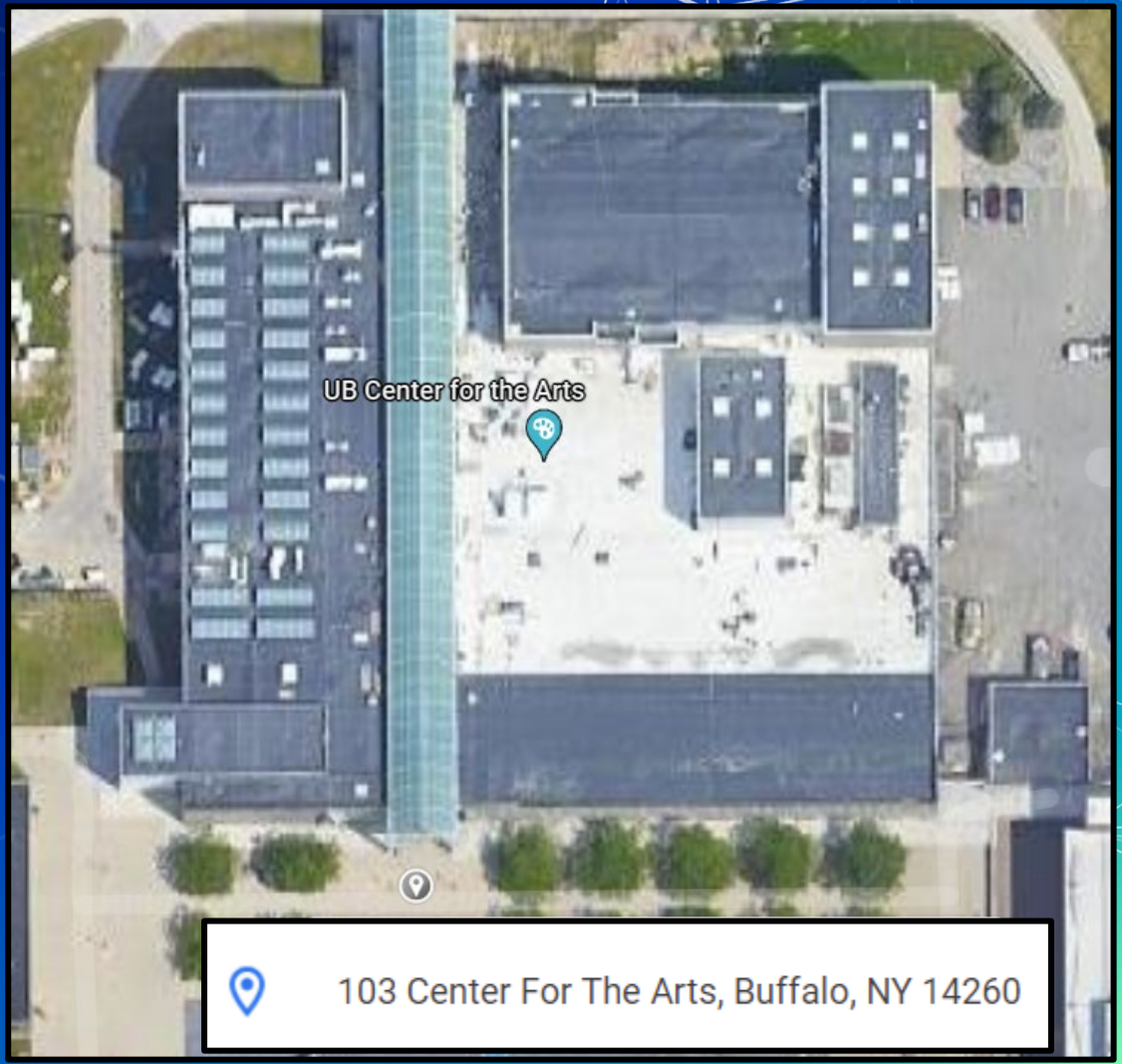
Intro to Ports

- Recall MAC Addresses
  - Eg. 00-10-FA-6E-38-4A
- Consider these similar to physical coordinates



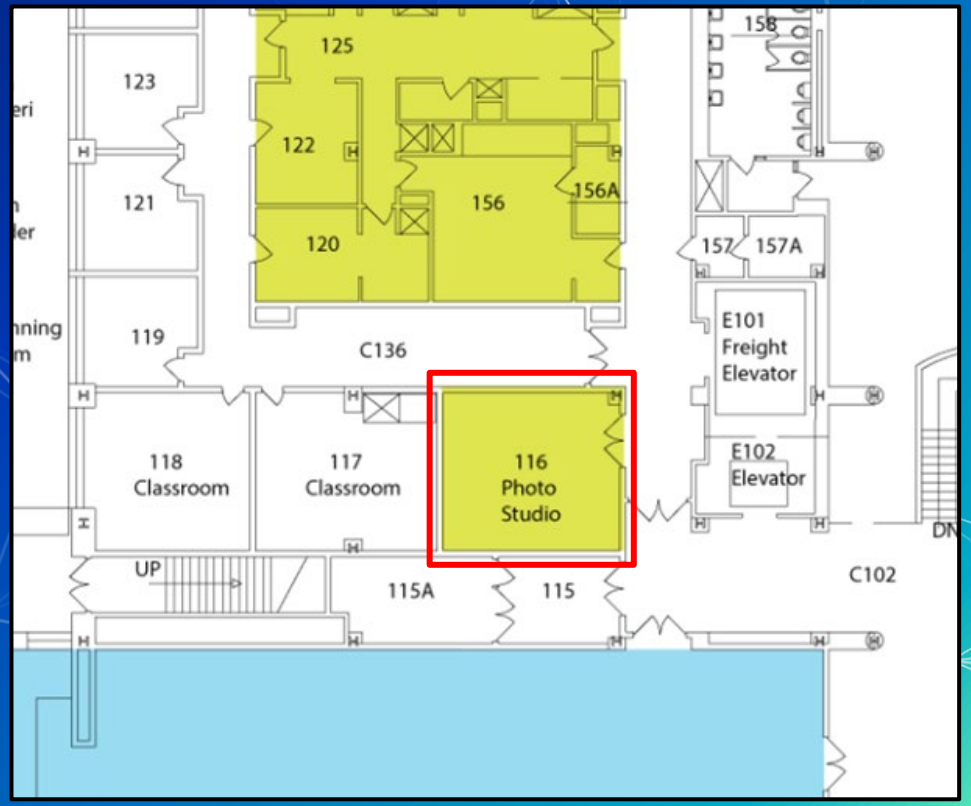
Intro to Ports

- Recall IP Addresses
- Consider these similar to postal addresses for buildings



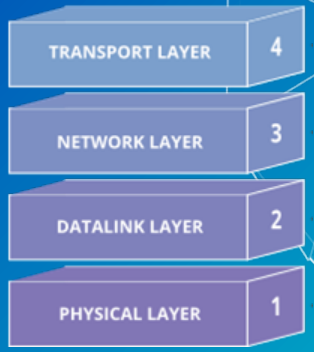
Intro to Ports

- Ports are similar to room numbers
  - MAC: 43.000483, -78.783078
  - IP: 103 Center for the Arts
  - Port: Room 116
- Ports are indicated next to IP addresses
  - 192.168.15.152**:116**



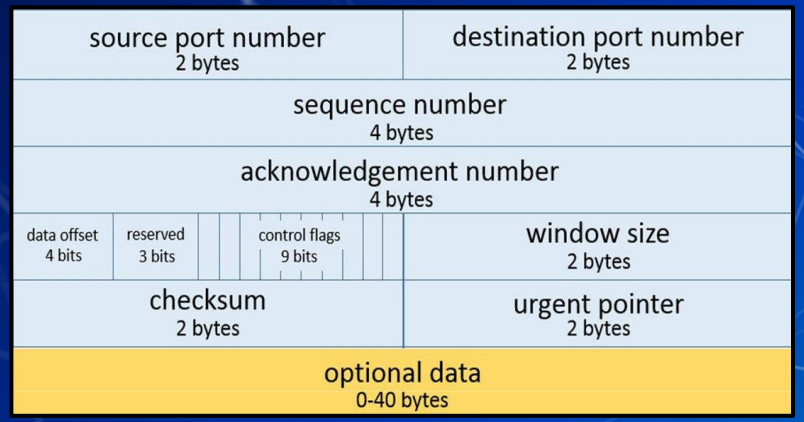
The Transport Layer

- Ports are managed by the OSI network transport layer
- The transport layer also manages packet exchange protocols
  - TCP
    - Downloading a File
  - UDP
    - Streaming or Video Call



Network Packet Headers

TCP Header



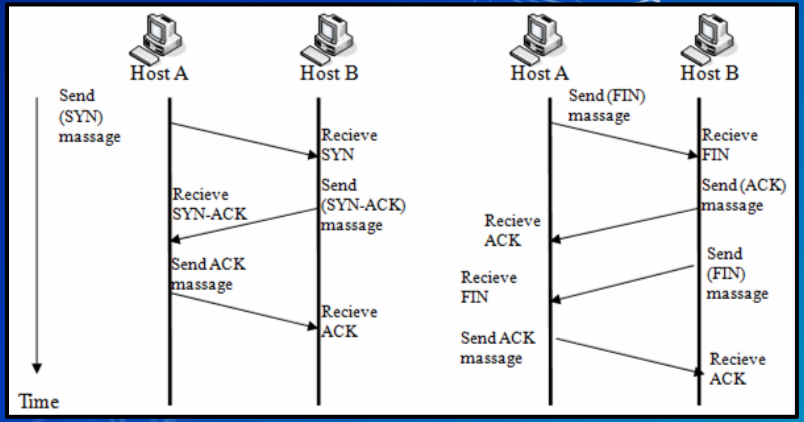
UDP Header

In Class Activity

TCP/UDP Packet Polo

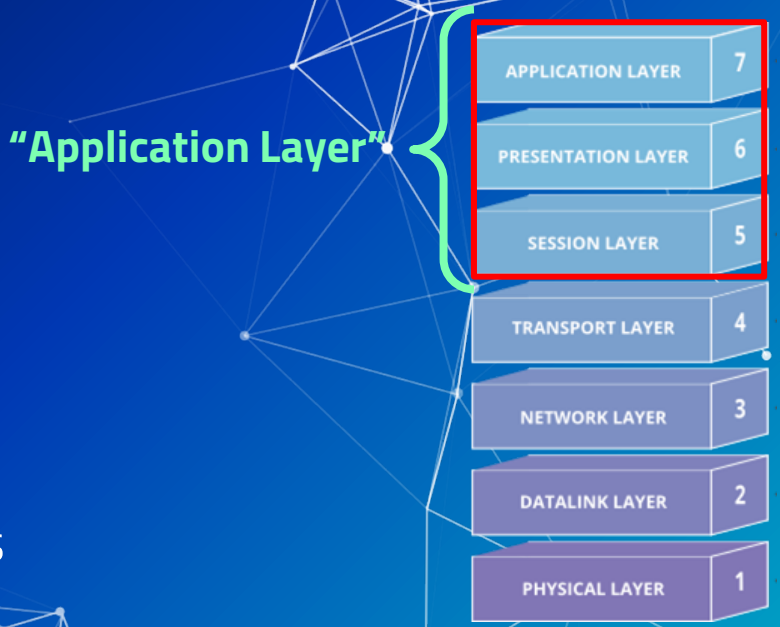
TCP Handshake

```
pfTop: Up State 1-100/114033, View: default, Order: bytes
PR        DIR SRC                        DEST                        STATE                 AGE       EXP     PKTS    BYTES
icmp      Out 192.168.253.18:17838       192.168.253.17:17838         0:0                 75:14:36  00:00:10  1060806 29702568
icmp      Out 192.168.253.18:42531       192.168.0.1:42531            0:0                 75:14:33  00:00:10  1060796 29702288
tcp       In  192.168.15.137:45602       192.168.253.18:80      ESTABLISHED:ESTABLISHED  00:01:51  23:59:55      983  1102747
tcp       In  192.168.15.137:45604       192.168.253.18:80      ESTABLISHED:ESTABLISHED  00:01:45  24:00:00      989   959986
tcp       In  10.3.1.70:61246            52.177.166.224:443     ESTABLISHED:ESTABLISHED  14:30:20  23:59:49     2654   352606
tcp       Out 192.168.253.18:52428       52.177.166.224:443     ESTABLISHED:ESTABLISHED  14:30:20  23:59:49     2654   352606
```



The Application Layer

- The transport layer cannot do it all
- For example:
  - Domain Name Service (DNS) Protocol
    - May require TCP or UDP protocols
  - Hypertext Transfer Protocol (HTTP)
    - Often requires two different devices
- Common port numbers are assigned to popular application protocols



Port #	Protocol
21	FTP Control
20	FTP Data
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS

DNS

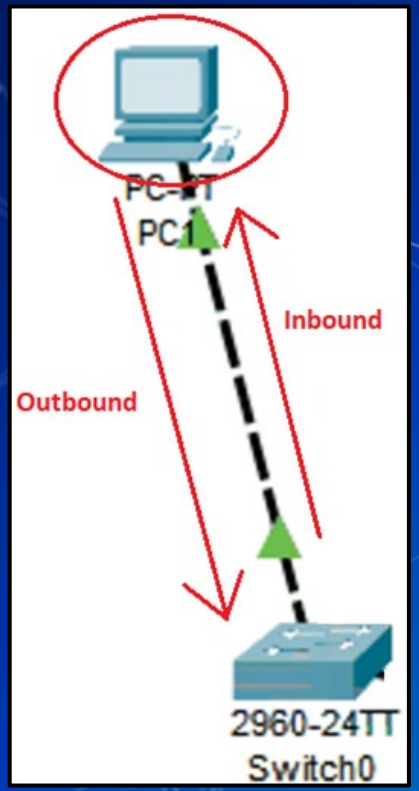
- How does your computer get to www.Google.com?
- A DNS server is used to translate a domain name to an IP address

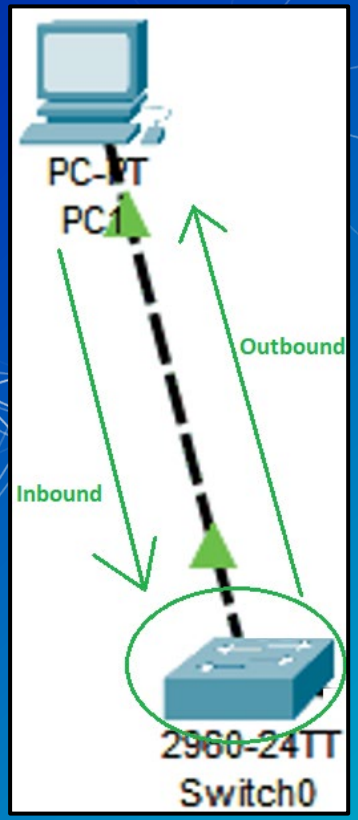
```
Name:     google.com
Addresses:  2607:f8b0:4006:81c::200e
          142.250.176.206
```

DNS Demo

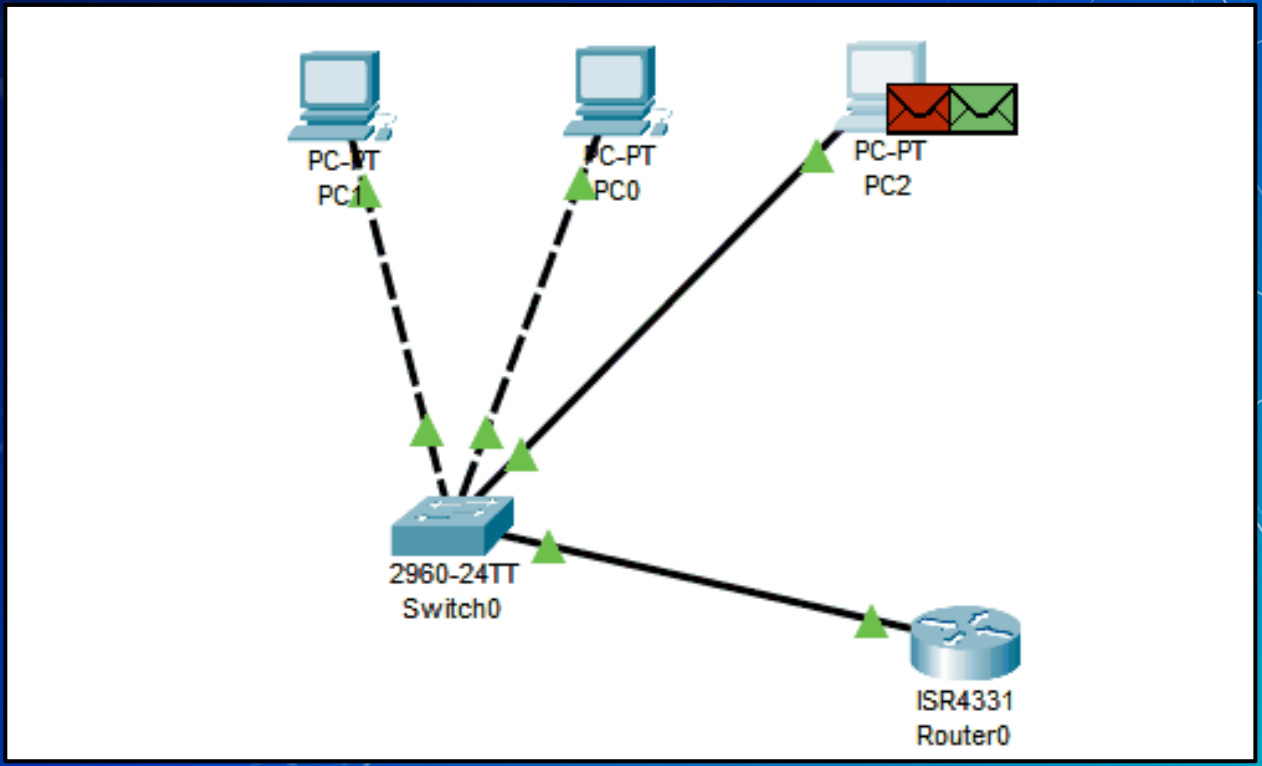
- Open a CLI
- `nslookup washington.edu`
- Copy IP Address into web browser
- You may need to use `http://` as a URL prefix

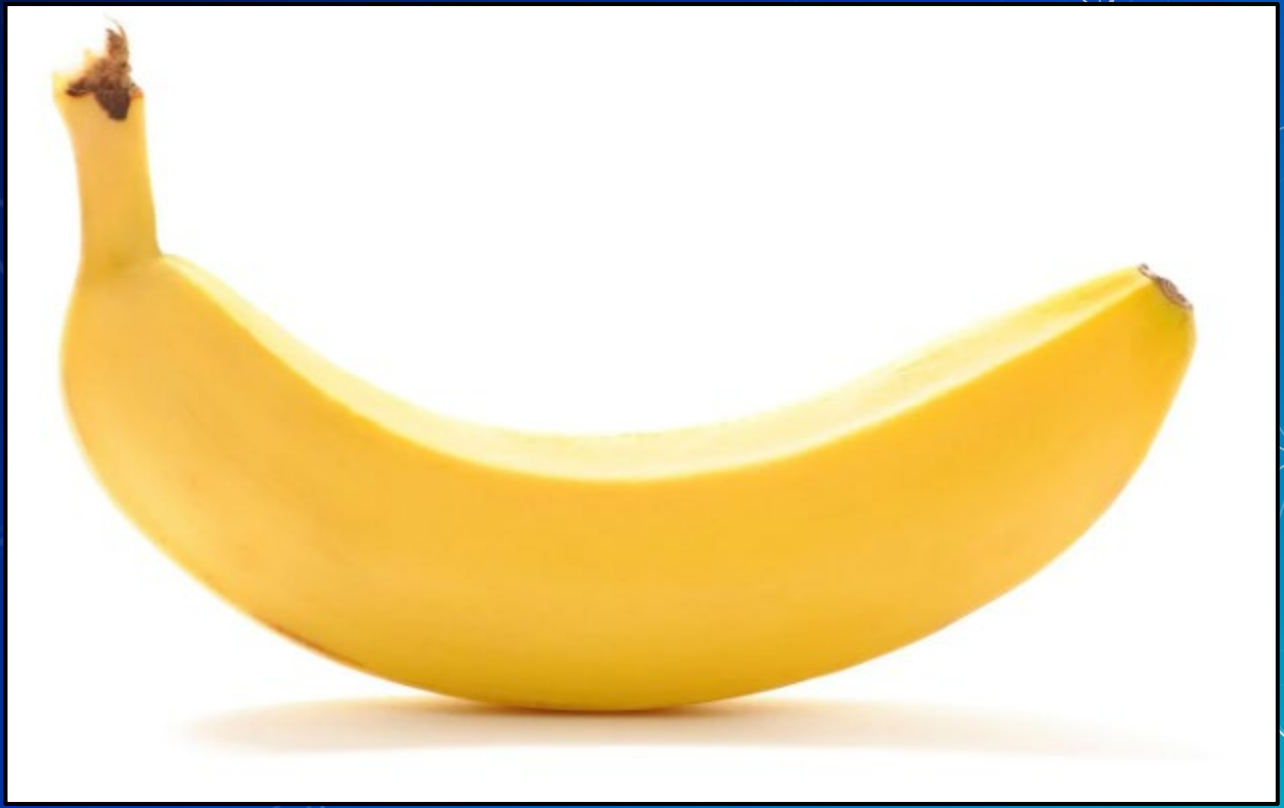
Directional Flow





Data flows freely... for now





Questions?

Agenda – Week 3

- Networking
  - Current Network State
  - Networking Part 2: Ports and Packets
  - In class exercise: TCP Packet Polo
- Migration Activity
- Firewalls
  - Types of Firewalls
  - In class exercise: TCP Packet Polo (with a firewall)
  - In class exercise: Login to pfSense
- Firewall and Packet Headers
- The Logic of Firewalls
  - How Traffic Flows
  - Default Rules
- pfSense Activity
- Homework Prep
- Summary/Wrap Up

In Class Activity

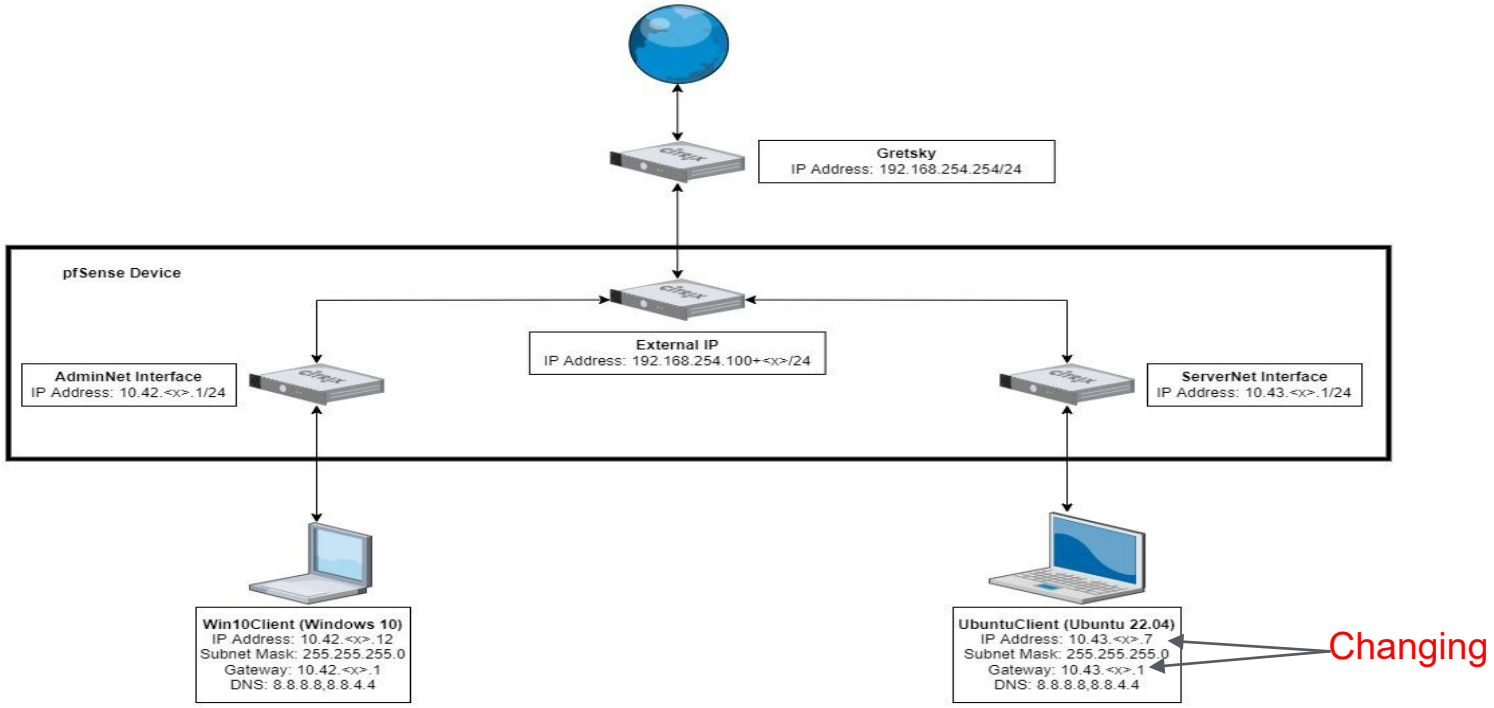
Hands-on Migration

Activity – Migrate Linux to `AdminNet`

- Migrate `UbuntuClient` from `ServerNet` to `AdminNet`.

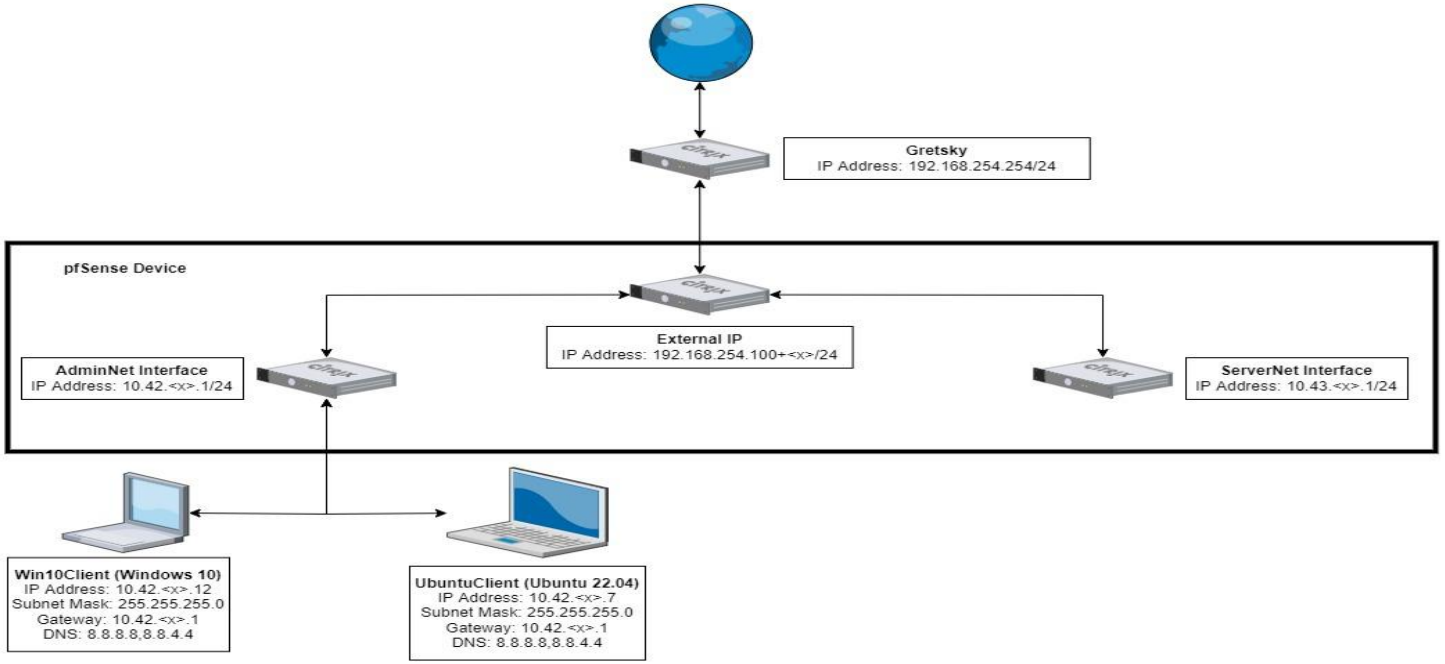
Activity – Migrate Linux to `AdminNet`

Before



Activity – Migrate Linux to `AdminNet`

After



Agenda – Week 3

- Networking
  - Current Network State
  - Networking Part 2: Ports and Packets
  - In class exercise: TCP Packet Polo
- Migration Activity
- Firewalls
  - Types of Firewalls
  - In class exercise: TCP Packet Polo (with a firewall)
  - In class exercise: Login to pfSense
- Firewall and Packet Headers
- The Logic of Firewalls
  - How Traffic Flows
  - Default Rules
- pfSense Activity
- Homework Prep
- Summary/Wrap Up

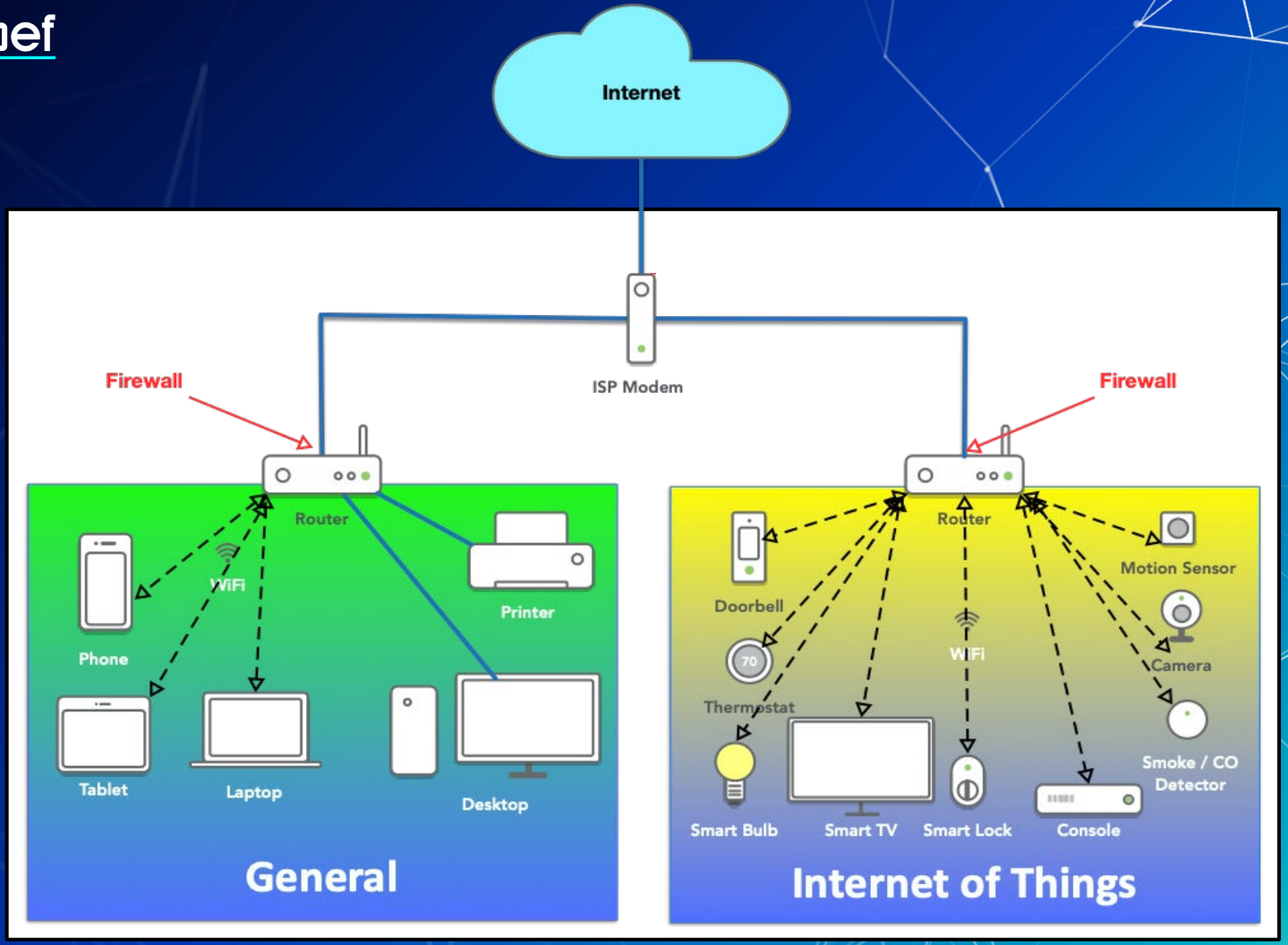
Types of Firewalls

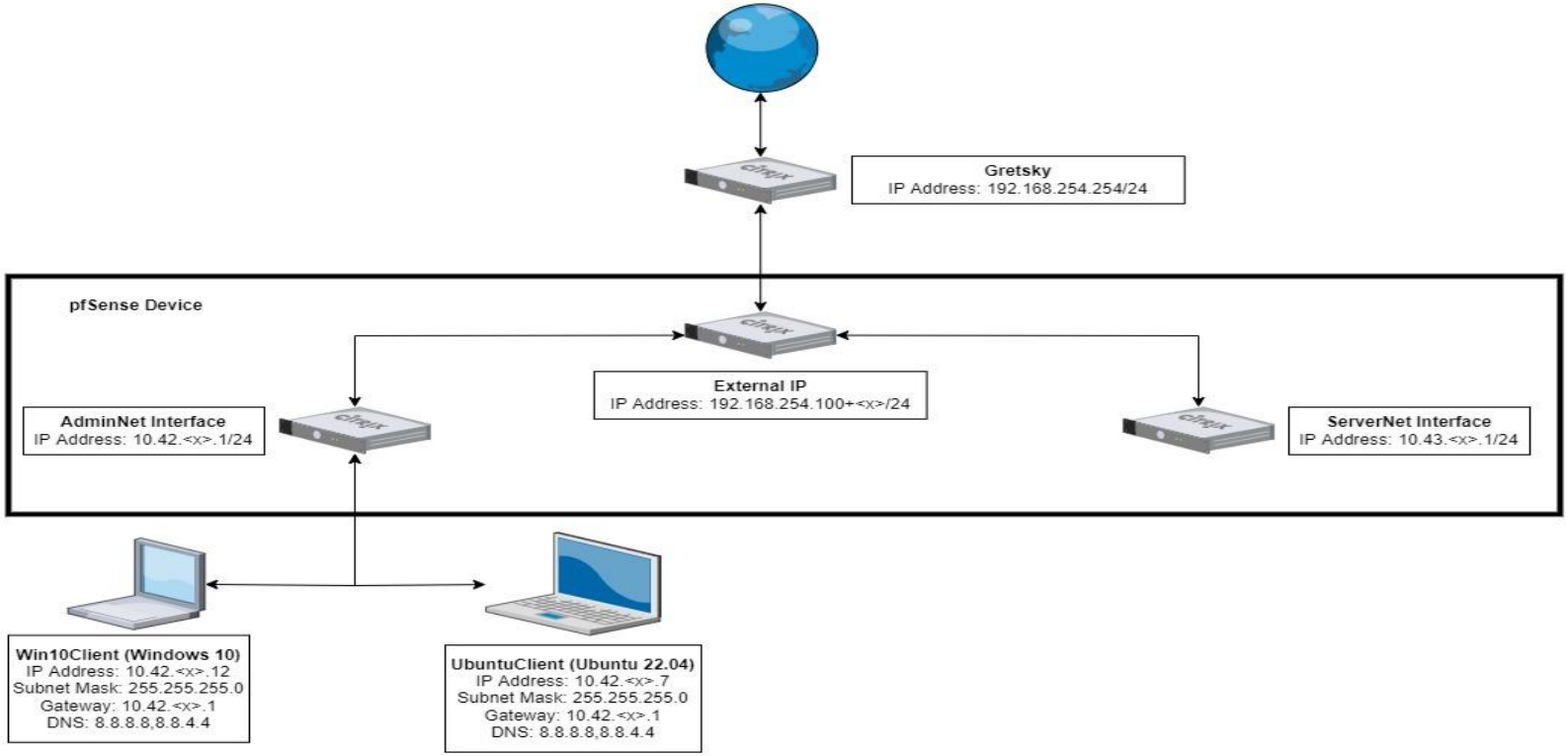
- Packet Filters (GEN 1)
- Stateful Firewalls (GEN 2)
- Next-generation Firewalls (NGFW)
  - Palo Alto (coming soon in this class)

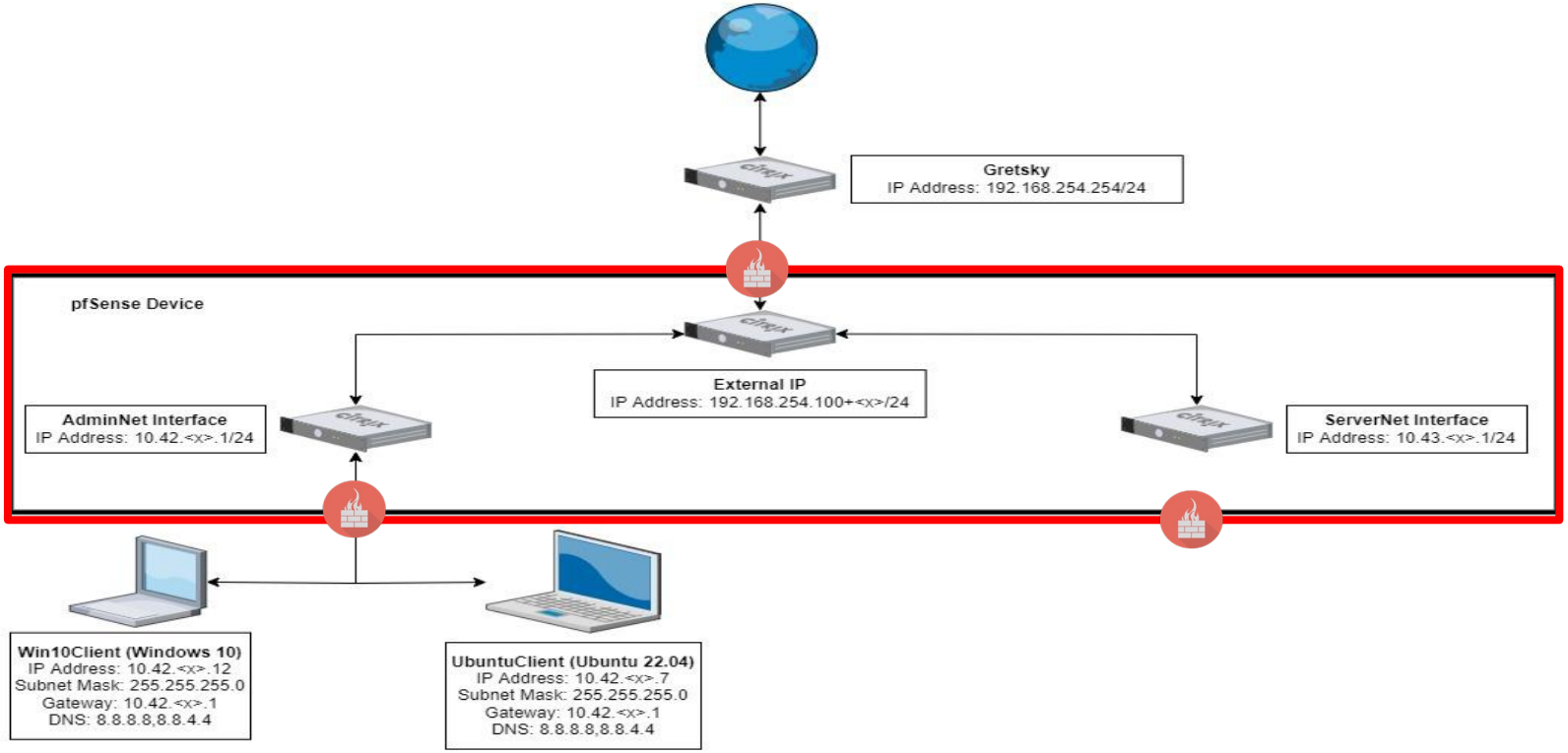
- Vantage Point
  - Network Perimeter
  - Host-Based

Why Firewalls?

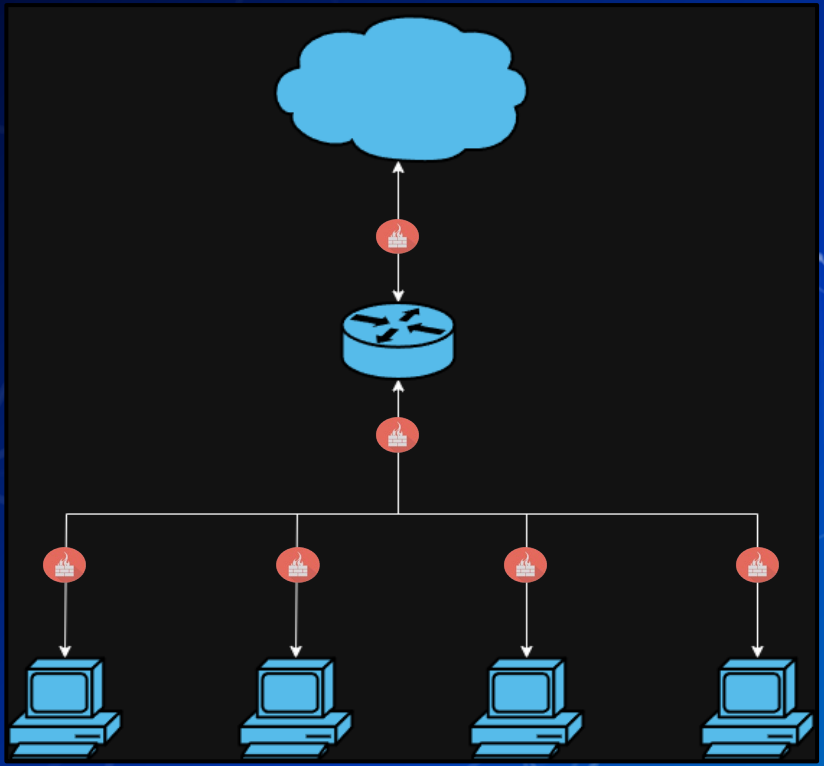
Any networked device can access the mission-critical system

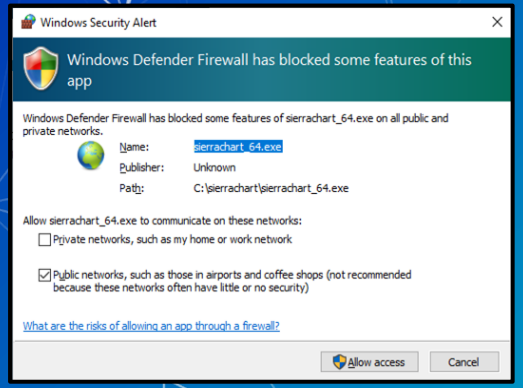

Internet
ISP Modem
Firewall
Firewall
Router
Router
WiFi
Phone
Tablet
Laptop
Desktop
Printer
General
Doorbell
Thermostat
70
Smart Bulb
Smart TV
Smart Lock
Console
WiFi
Motion Sensor
Camera
Smoke / CO
Detector
Internet of Things


Gretsky
IP Address: 192.168.254.254/24
pfSense Device
External IP
IP Address: 192.168.254.100+<x>/24
AdminNet Interface
IP Address: 10.42.<x>.1/24
ServerNet Interface
IP Address: 10.43.<x>.1/24
Win10Client (Windows 10)
IP Address: 10.42.<x>.12
Subnet Mask: 255.255.255.0
Gateway: 10.42.<x>.1
DNS: 8.8.8.8,8.8.4.4
UbuntuClient (Ubuntu 22.04)
IP Address: 10.42.<x>.7
Subnet Mask: 255.255.255.0
Gateway: 10.42.<x>.1
DNS: 8.8.8.8,8.8.4.4


Gretsky
IP Address: 192.168.254.254/24
pfSense Device
External IP
IP Address: 192.168.254.100+<x>/24
AdminNet Interface
IP Address: 10.42.<x>.1/24
ServerNet Interface
IP Address: 10.43.<x>.1/24
Win10Client (Windows 10)
IP Address: 10.42.<x>.12
Subnet Mask: 255.255.255.0
Gateway: 10.42.<x>.1
DNS: 8.8.8.8,8.8.4.4
UbuntuClient (Ubuntu 22.04)
IP Address: 10.42.<x>.7
Subnet Mask: 255.255.255.0
Gateway: 10.42.<x>.1
DNS: 8.8.8.8,8.8.4.4

Host based Firewalls



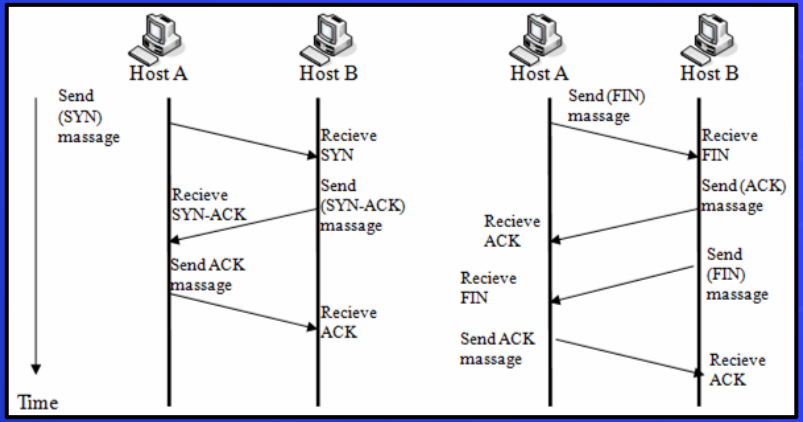



```
root@nixcraft:~#
root@nixcraft:~# iptables -A INPUT -s 202.54.1.1 -j DROP -m comment --comment "DROP spam IP address"
root@nixcraft:~#
root@nixcraft:~# iptables -L INPUT -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:53 /* generated for LXD network lxdbr0 */
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53 /* generated for LXD network lxdbr0 */
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:67 /* generated for LXD network lxdbr0 */
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:67
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:67
DROP       all  --  202.54.1.1           0.0.0.0/0            /* DROP spam IP address */
root@nixcraft:~#
root@nixcraft:~#
root@nixcraft:~# iptables -A INPUT -p tcp --dport 80 -m comment --comment "block HTTPD access" -j DROP
root@nixcraft:~# iptables -A INPUT -p tcp --dport 443 -m comment --comment "block HTTPDS access" -j DROP
root@nixcraft:~#
root@nixcraft:~# iptables -L INPUT -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:53 /* generated for LXD network lxdbr0 */
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53 /* generated for LXD network lxdbr0 */
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:67 /* generated for LXD network lxdbr0 */
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:67
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:67
DROP       all  --  202.54.1.1           0.0.0.0/0            /* DROP spam IP address */
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:80 /* block HTTPD access */
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:443 /* block HTTPDS access */
```

In Class Activity

TCP/UDP Packet Polo with Firewall

TCP/UDP Packet Polo with Firewall



Break slide

Please return in 10 minutes

In Class Activity

Login to pfSense

Accessing pfSense

- Open Win10Client
- Open a browser of your choice and a CLI
- Run command `ipconfig`
- Type the IP of the “default gateway” device into the address bar of your browser
- The credentials for pfSense will be `admin` as the user and the password is `pfsense`

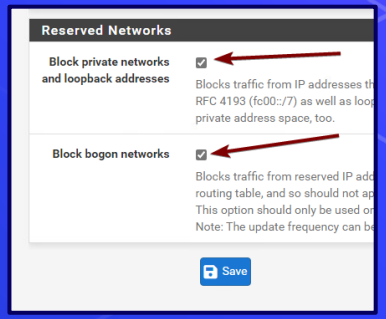
Disabling Default WAN(External) Firewall Rules

- Select the Firewalls dropbox at the top of the menu and select rules
- Click on the gear

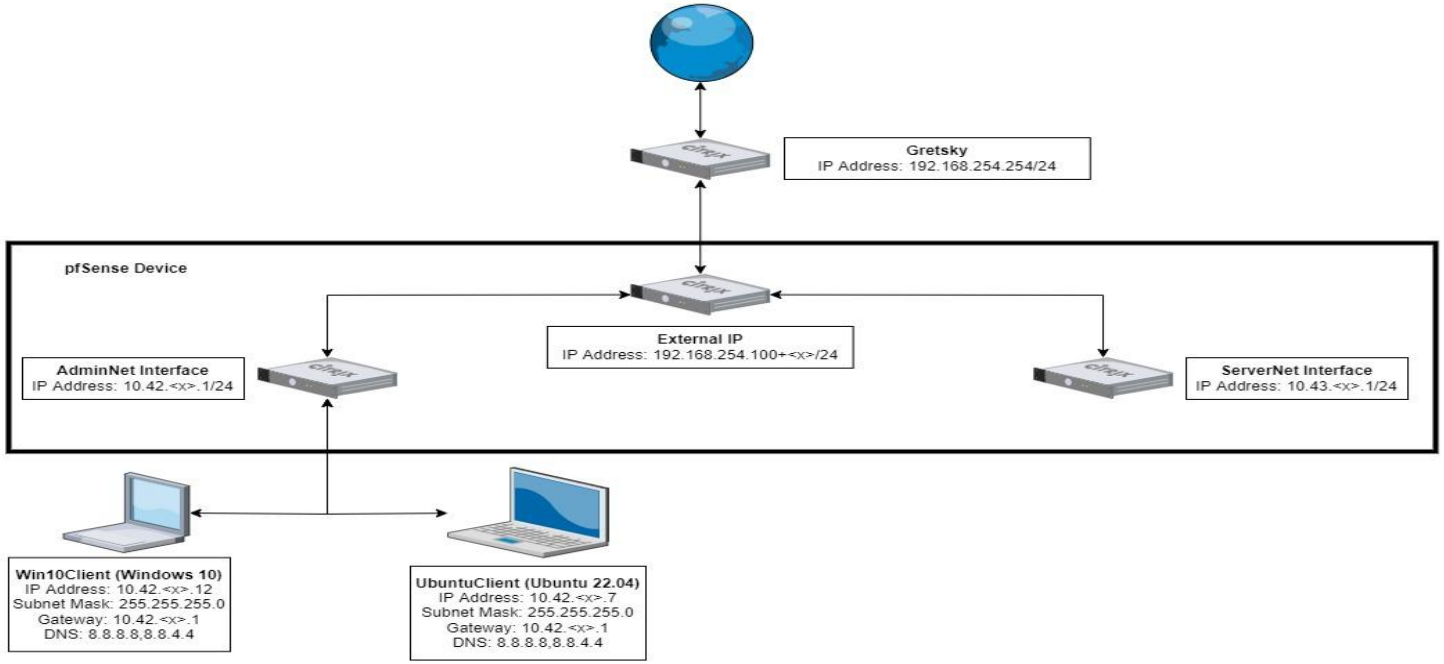
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✕	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
✕	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

- Scroll to the bottom and uncheck the two checkboxes
- Don’t forget to save at the bottom and by pressing apply changes



Reminder: Current Network State



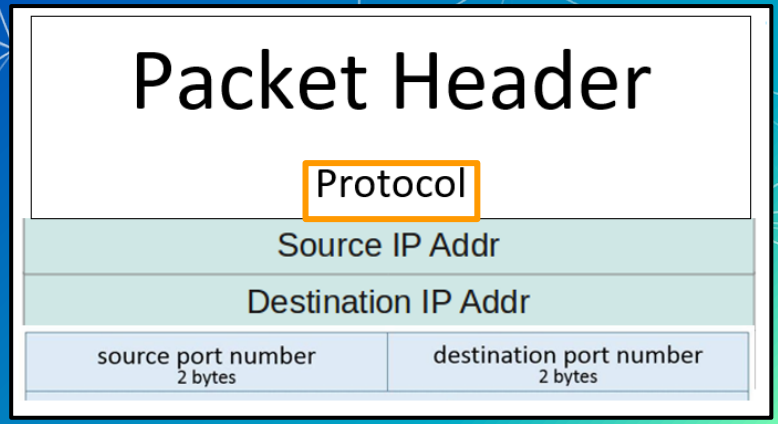
Agenda – Week 3

- Networking
  - Current Network State
  - Networking Part 2: Ports and Packets
  - In class exercise: TCP Packet Polo
- Migration Activity
- Firewalls
  - Types of Firewalls
  - In class exercise: TCP Packet Polo (with a firewall)
  - In class exercise: Login to pfSense
- Firewall and Packet Headers
- The Logic of Firewalls
  - How Traffic Flows
  - Default Rules
- pfSense Activity
- Homework Prep
- Summary/Wrap Up

Header to Firewall

Rules (Drag to Change Order)

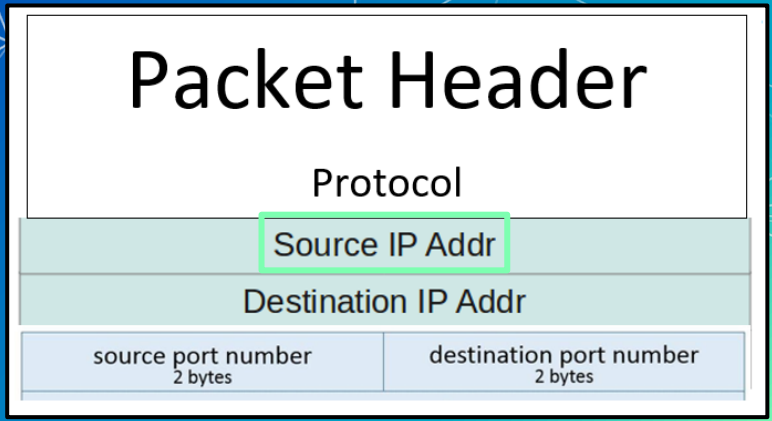
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
☐	✓	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
☐	✓	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
☐	✗	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			



Header to Firewall

Rules (Drag to Change Order)

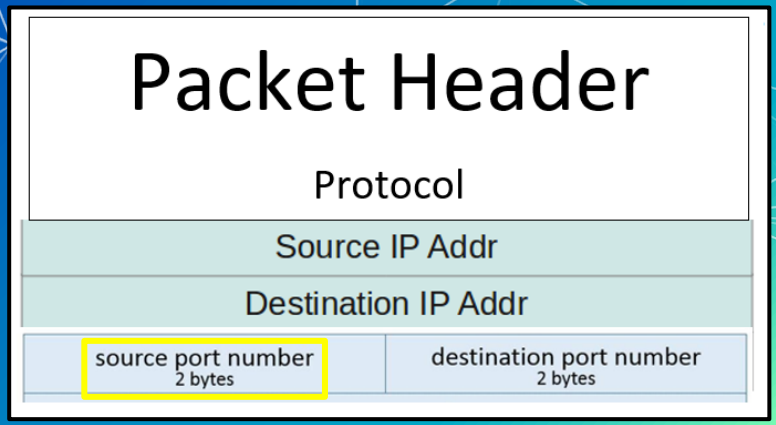
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
✓	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
✓	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
✗	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			



Header to Firewall

Rules (Drag to Change Order)

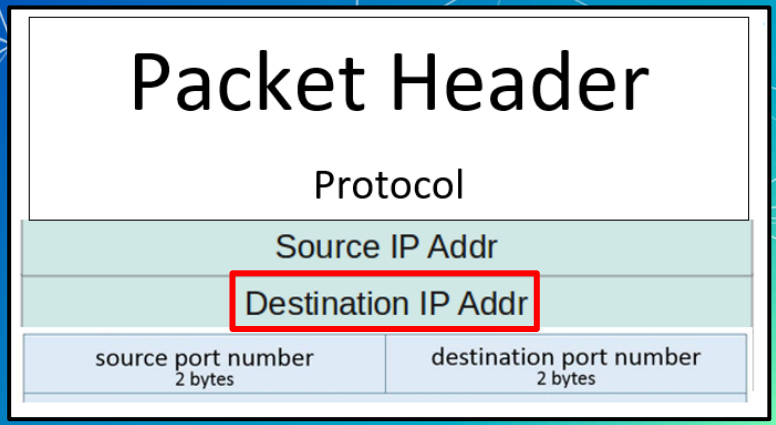
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
☐	✓	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
☐	✓	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
☐	✗	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			



Header to Firewall

Rules (Drag to Change Order)

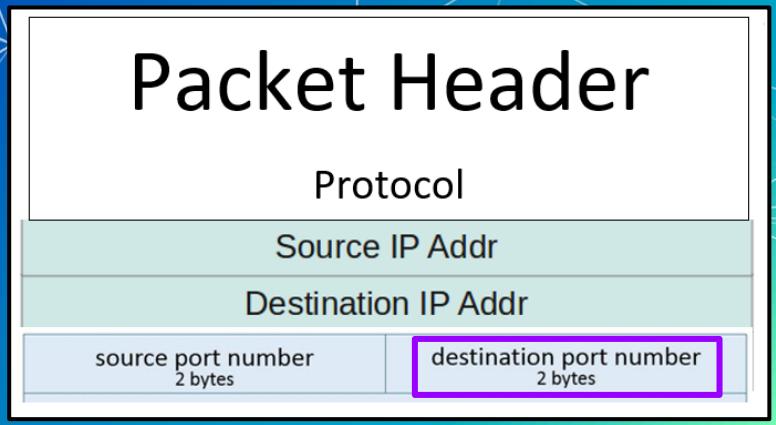
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
✓	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
✓	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
✗	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			



Header to Firewall

Rules (Drag to Change Order)

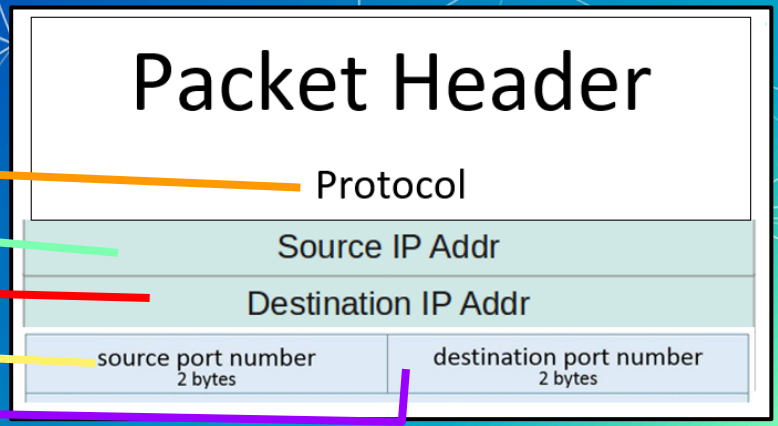
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
☐	✓	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
☐	✓	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
☐	✗	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			



Header to Firewall

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
☐	✓	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
☐	✓	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
☐	✗	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			



Agenda – Week 3

- Networking
  - Current Network State
  - Networking Part 2: Ports and Packets
  - In class exercise: TCP Packet Polo
- Migration Activity
- Firewalls
  - Types of Firewalls
  - In class exercise: TCP Packet Polo (with a firewall)
  - In class exercise: Login to pfSense
- Firewall and Packet Headers
- The Logic of Firewalls
  - How Traffic Flows
  - Default Rules
- pfSense Activity
- Homework Prep
- Summary/Wrap Up

The Logic of Firewalls

Rule Hierarchy

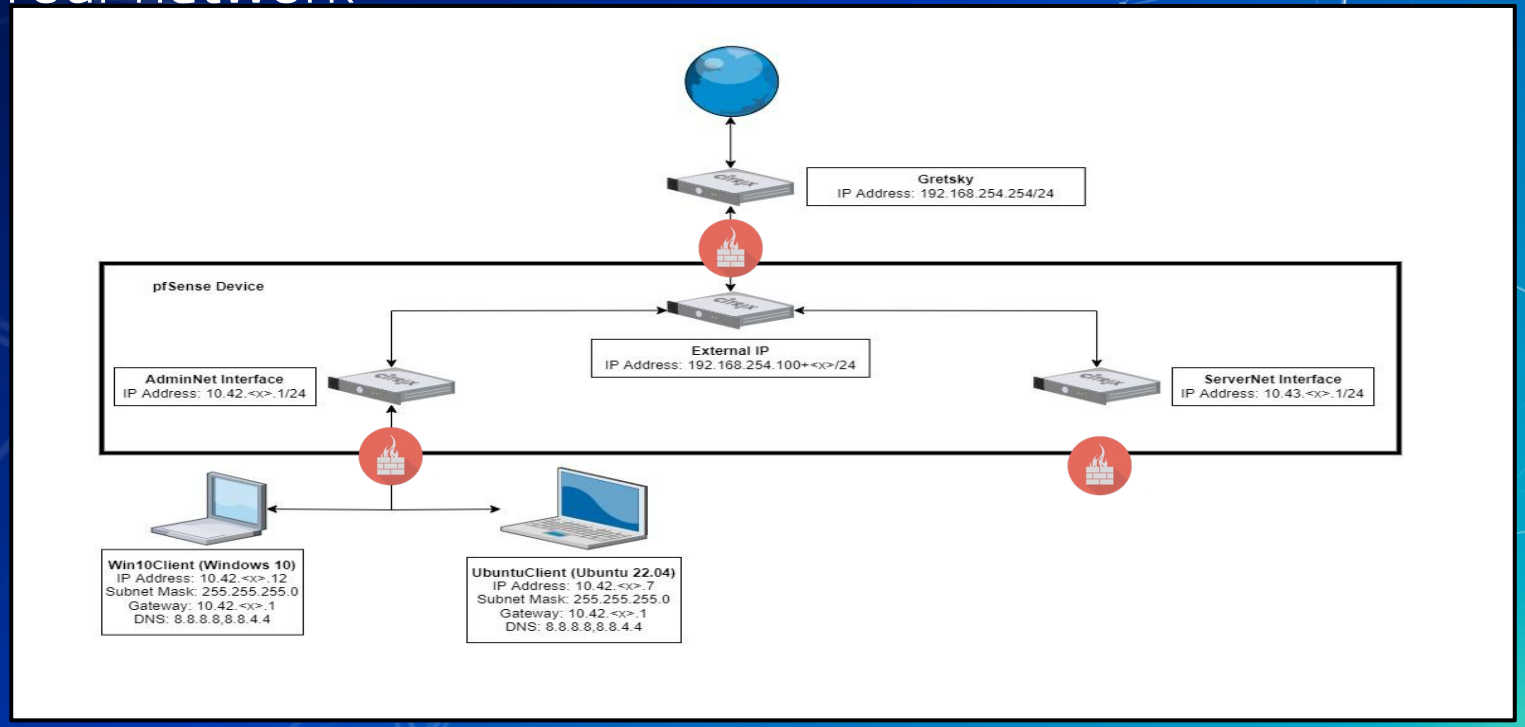
- Each packet is checked against rules.
  - Rules are enforced from top to bottom
    - Packets can be:
      - Rejected
      - Dropped
      - Allowed

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✔	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
☐	✔	0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
☐	✔	0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
☐	✘	0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			

How Traffic Flows

- Your network



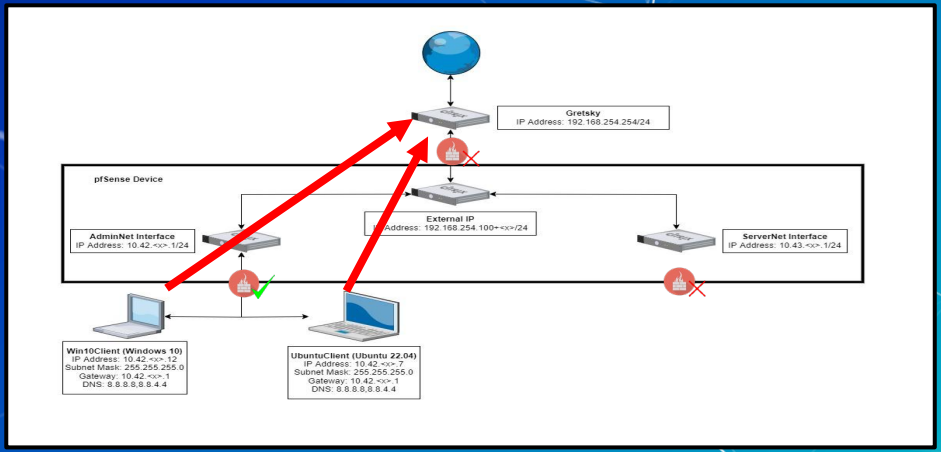
How Traffic Flows

- From LAN (AdminNet) to Web

Floating WAN LAN OPT1

Rules (Drag to Change Order)

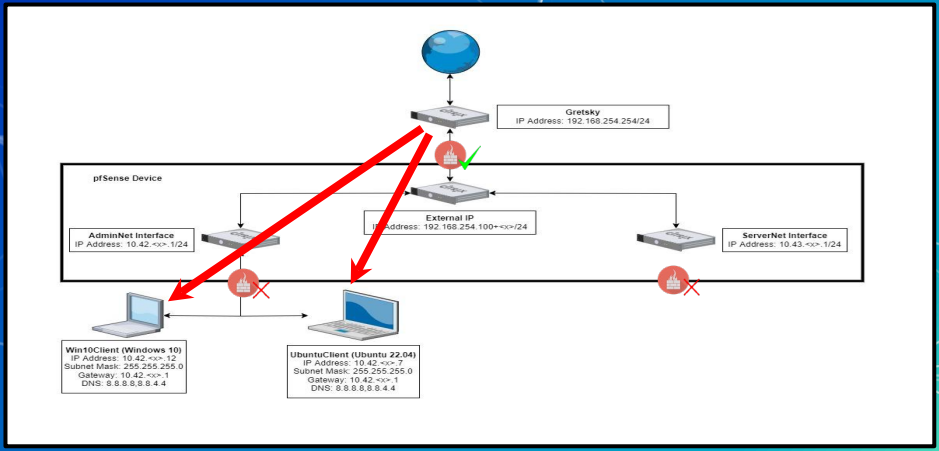
	States	Protocol	Source	Port	Destination	Port	Gateway
✔	0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*



How Traffic Flows

- From Web to LAN (`AdminNet`)
- Web inbound is managed by the WAN (`External`) interface

Floating | WAN | LAN | OPT1



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway
✓	2 /249 KiB	IPv4 TCP	192.168.13.71	*	10.42.29.11	3389	*

Default rule

- What if a packet doesn’t match any of our rules?

Default rule

- What if a packet doesn't match any of our rules?
  - Firewalls use one or more default "catch all rule(s)" that is enforced when a packet does not match any listed rules.
  - The default behavior depends on firewall manufacturer

Define Your Own Default Rule(s)

- Self defined default firewall rule(s) need to be at the bottom of the firewall's rule list
- What are the advantages of the default rules seen below?

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
✖	0 /2 KiB	IPv4+6 *	*	*	*	*	*	none

✔	5 /7.08 MiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule
✔	0 /0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule

Logic of Firewalls
Questions?

Agenda – Week 3

- Networking
  - Current Network State
  - Networking Part 2: Ports and Packets
  - In class exercise: TCP Packet Polo
- Migration Activity
- Firewalls
  - Types of Firewalls
  - In class exercise: TCP Packet Polo (with a firewall)
  - In class exercise: Login to pfSense
- Firewall and Packet Headers
- The Logic of Firewalls
  - How Traffic Flows
  - Default Rules
- pfSense Activity
- Homework Prep
- Summary/Wrap Up

In Class Activity

pfSense Hands-On

Activity – pfSense Firewall

- Login to pfSense and follow along.
- Create rules to allow Ping, HTTP, and HTTPS from LAN to anywhere.
- Edit default Allow rule to Deny all traffic out of LAN (Place this rule on the bottom as a catch-all).

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /2.60 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✗	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default block LAN to any rule	
✗	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default block LAN IPv6 to any rule	

Activity – Tricky Traffic

- What's being blocked by the Default Deny All?
- Hint[0]: `ping 8.8.8.8` and `ping google.com`
- Hint[1]: How can we see if a rule is being hit.
- Hint[2]: Is there a way to log traffic getting caught by a rule?

Homework Prep

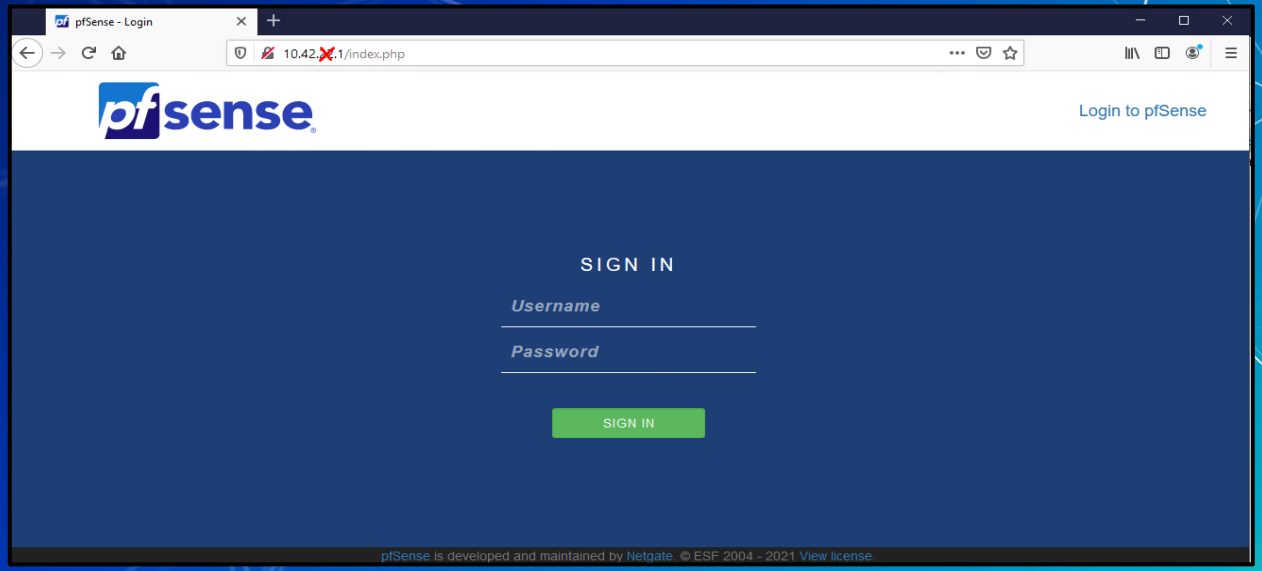
System Prep

- Prep 1: Install SSH on your Linux client
  - Package name: openssh-server
    - `sudo apt install openssh-server`
    - https://youtu.be/HJXo68LnNOs
- Prep 2: Run script from GitHub on Windows Client (PrepareWindowsSystem.ps1)
  - https://github.com/ubnetdef/WindowsScriptsForLecture
  - https://www.youtube.com/watch?v=Z6kNyfZiNxg

Homework Starter

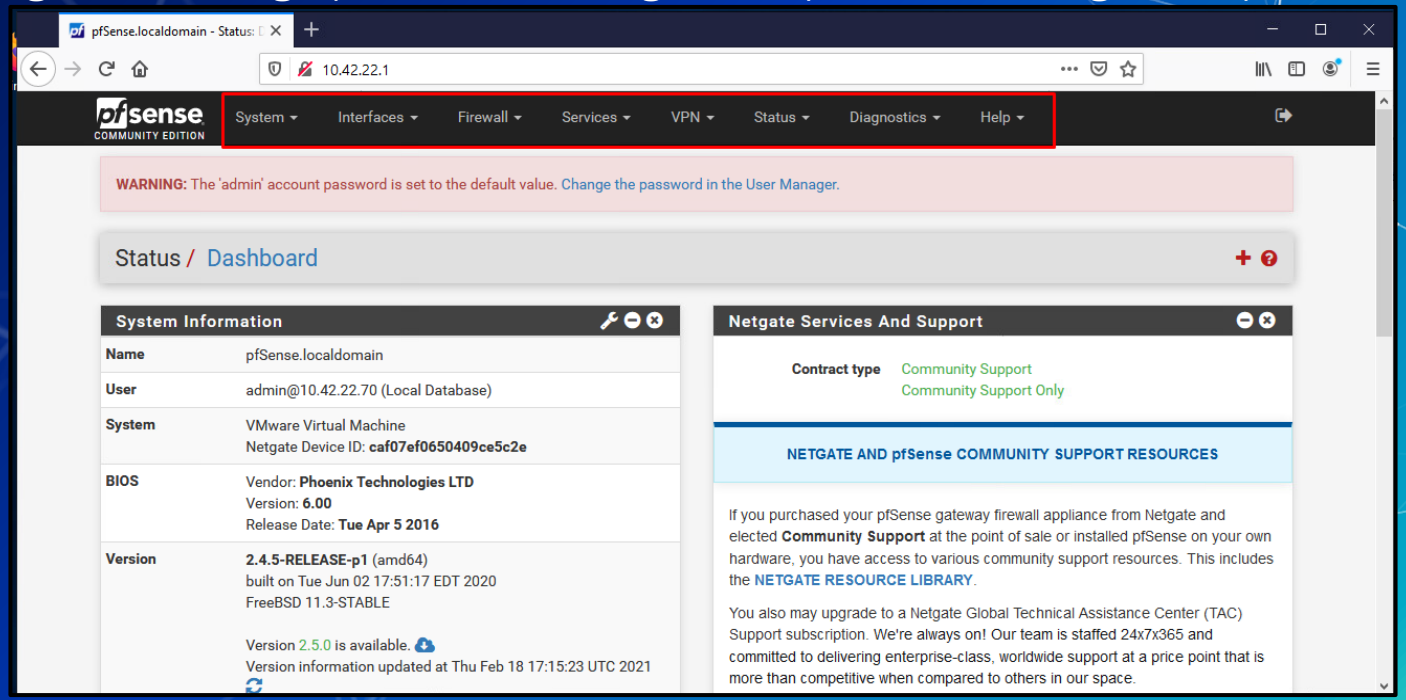
Homework Starter

- Credentials
  - Username: `admin`
  - Password: `pfsense`



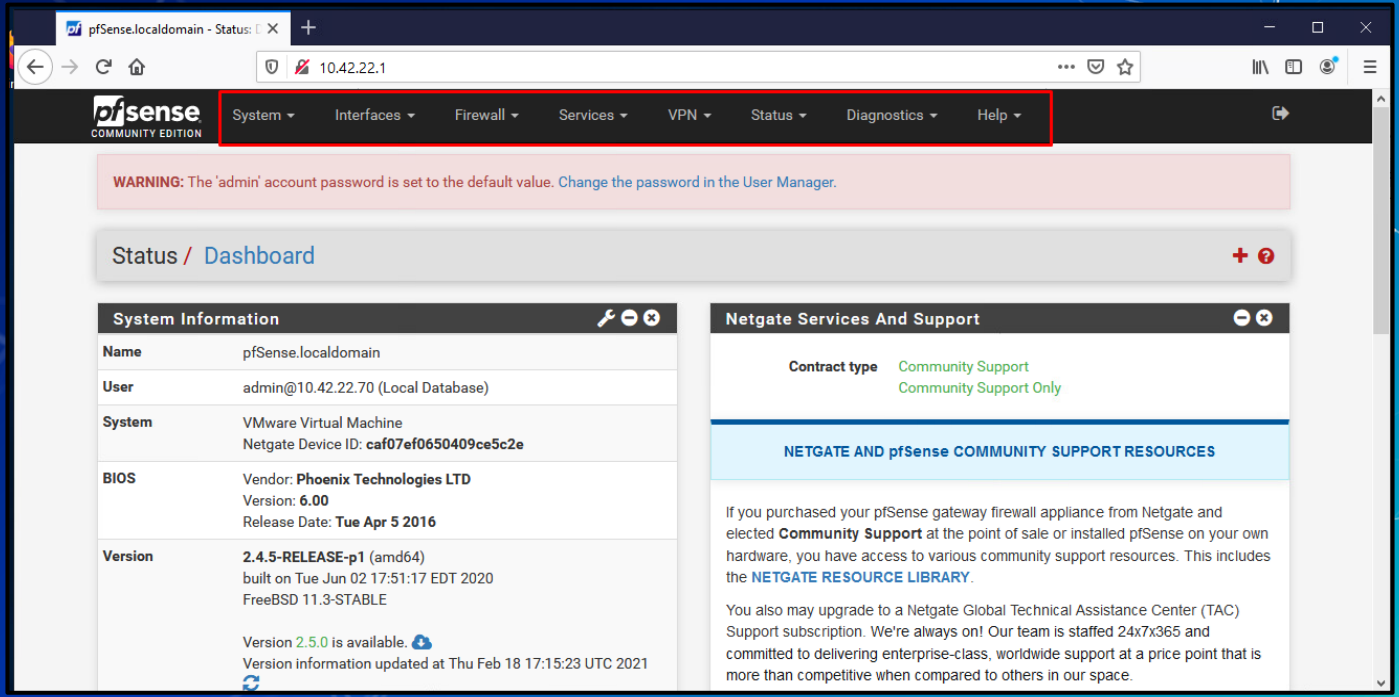
Homework Starter

- Navigation through pfSense UI can generally be done using the top bar



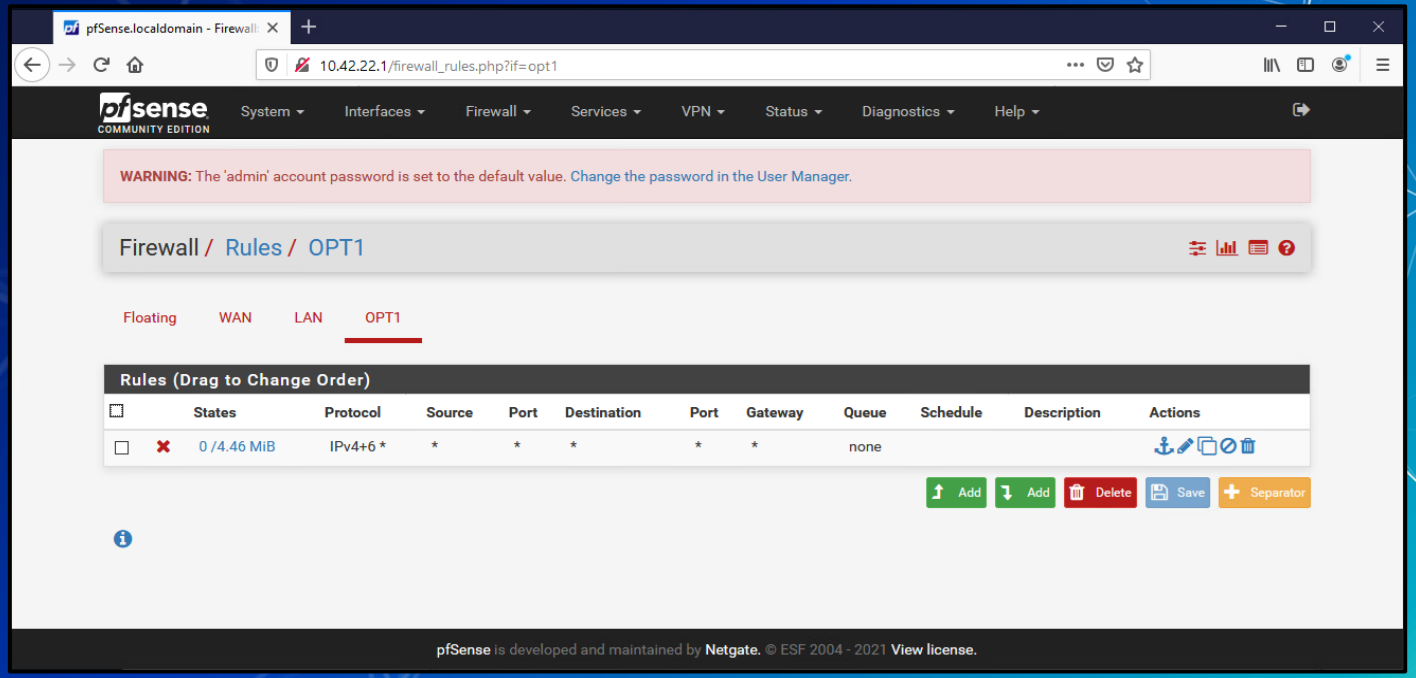
Homework Starter

- Rules menu is under `Firewall > Rules`



Homework Starter

- Rules are grouped by the interface that handles the packets



Homework Hint

- If after you apply a firewall rule you can no longer connect to your pfsense router through the Web Interface it is likely you have a firewall rule that is blocking you.
  - Use `pfctl -d` to disable the firewall and make sure to fix the offending rule before applying and additional rules.
- Everytime you modify any rule and commit the change your firewall will be reenabled
- Changing one rule at a time and testing may be best practice

Summary and Wrap-up

Today's achievements:

- Reviewed networking
- Further dive into OSI model specifically in the transport layer with the TCP handshake and UDP
- Migrated UbuntuClient to AdminNet
- Learned about firewalls and the different types
- Configured firewall rules to block a compromised device

Parting Questions

Class dismissed

See you next week!