

Firewalls

UBNetDef, Fall 2022
Week 3

Lead Presenter:
Raymond Harenza

Networking Part 2

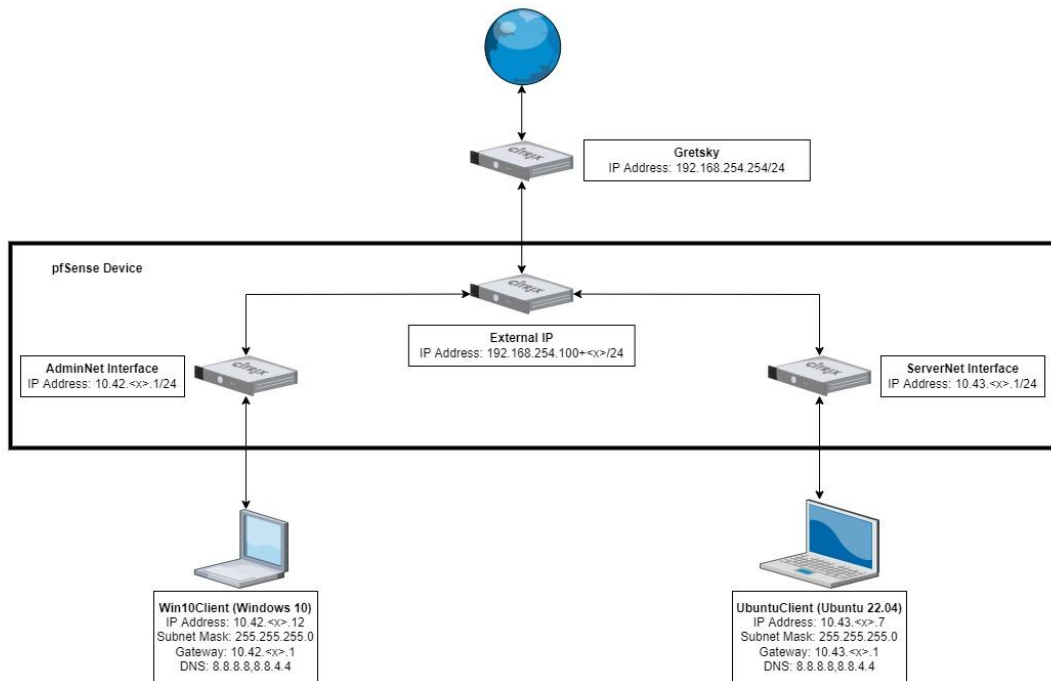
Learning Objectives

- 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

- Reviewing current network state
- Networking Part 2 with Ports
- Hands-on Activity 1
- The Application layer
- Domain Name Service Demo
- Directional Flow
- Hands-on Activity 2
- The Logic of Firewalls
- Homework System Prep

Current Network State



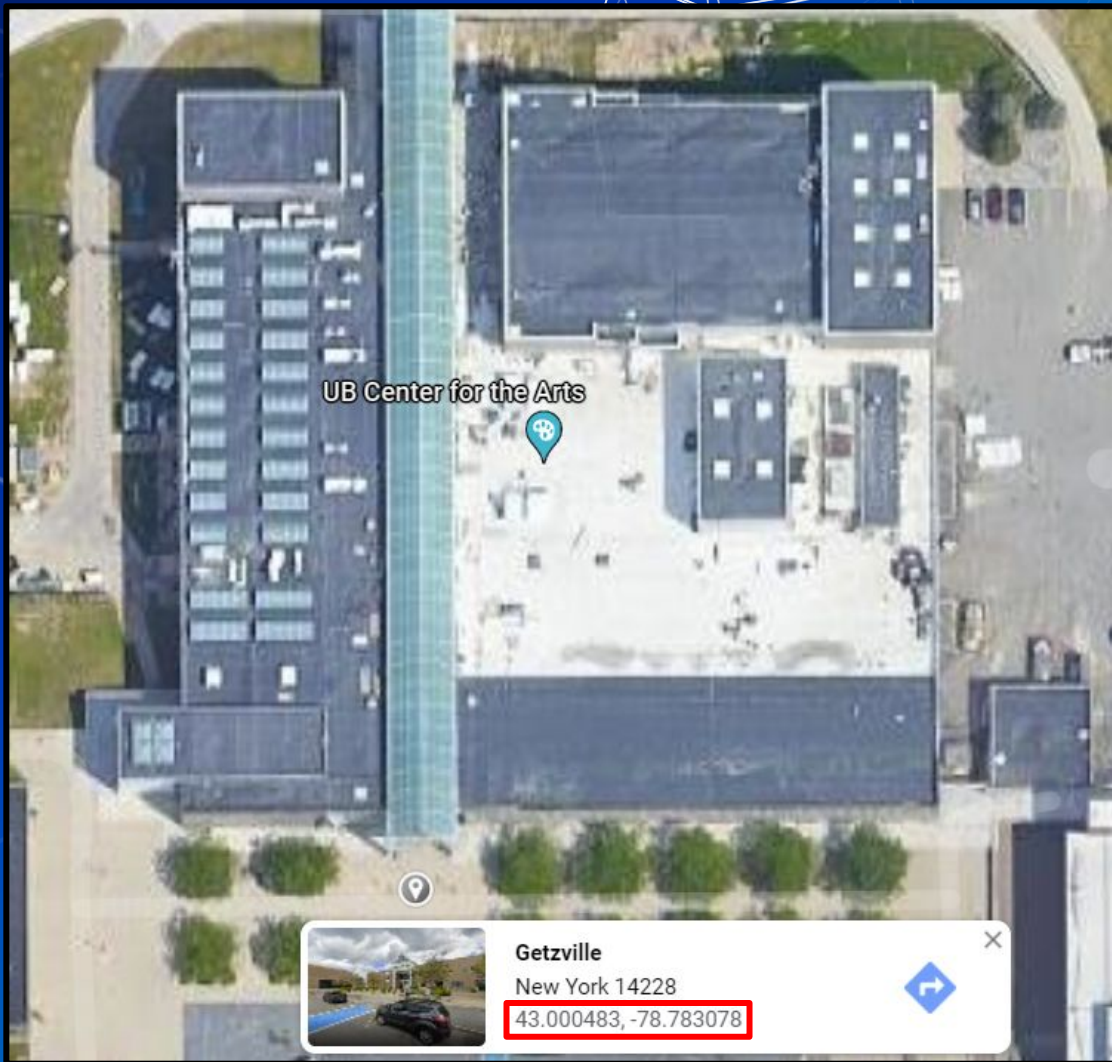
Networking Part 2

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



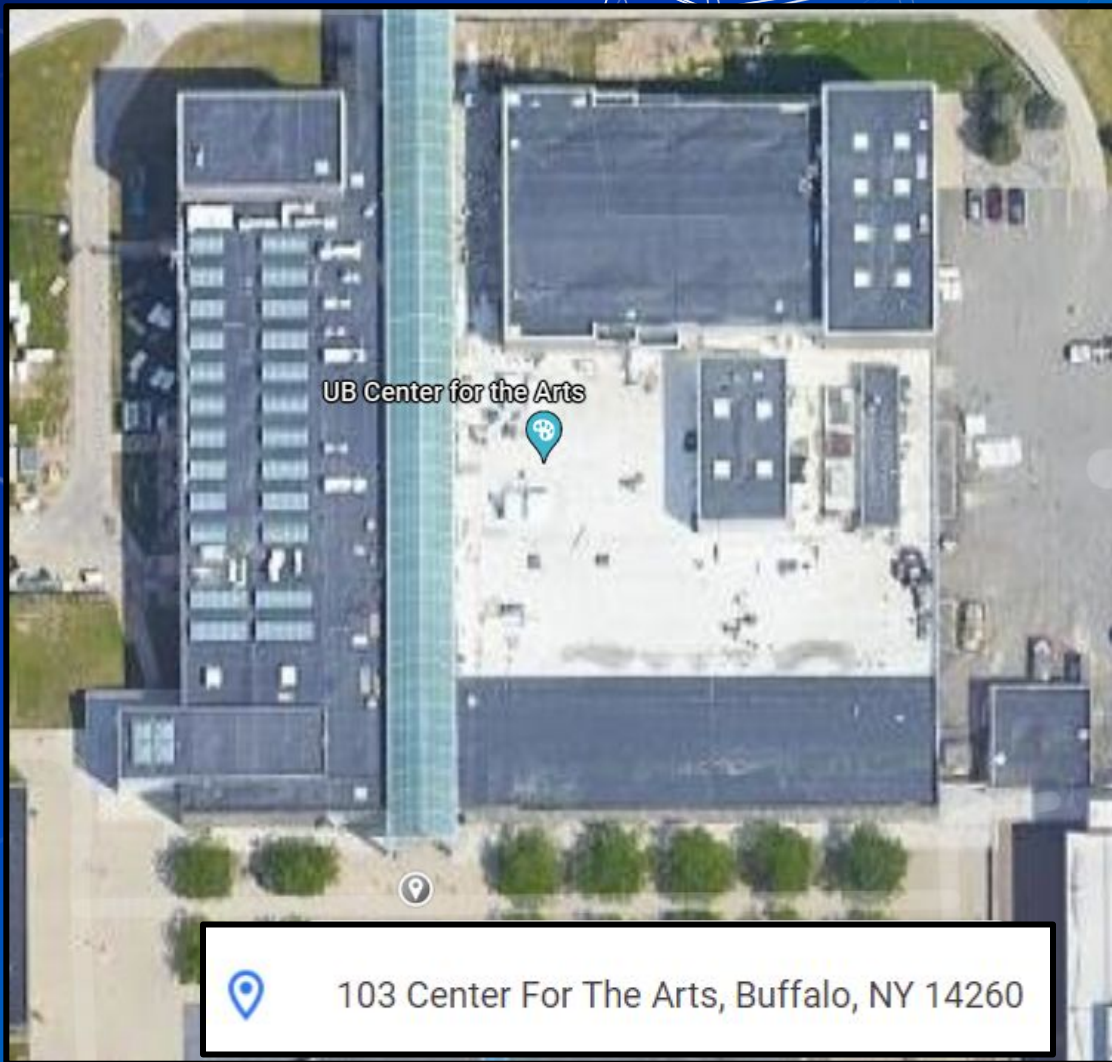
Intro to Ports

- Recall MAC Addresses
- Consider these similar to physical coordinates



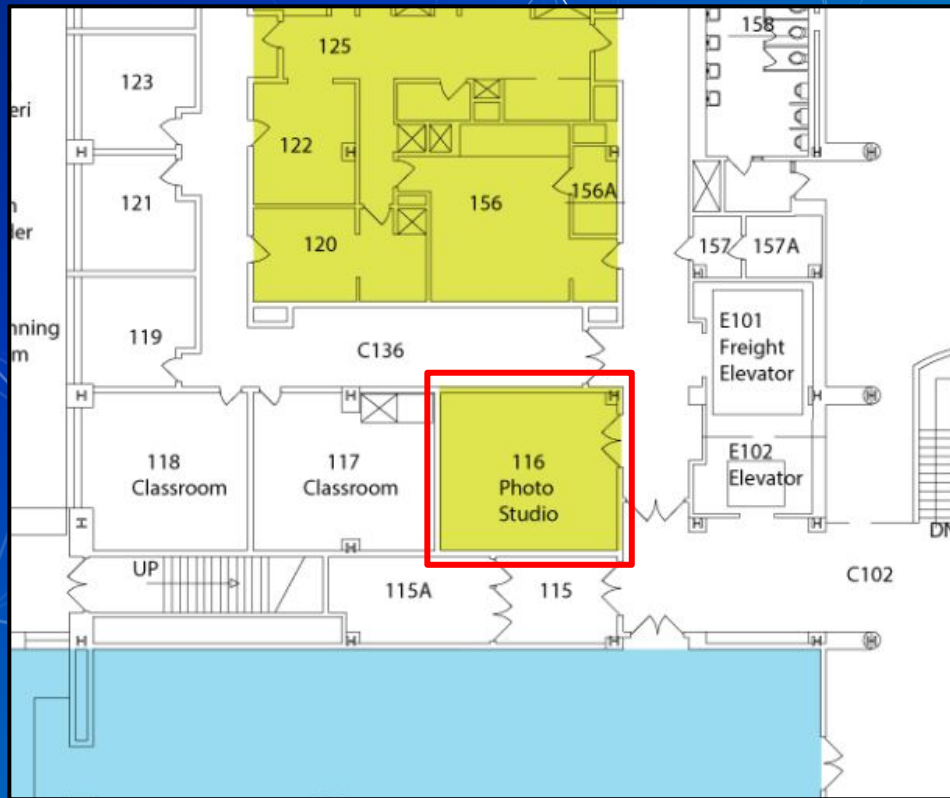
Intro to Ports

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

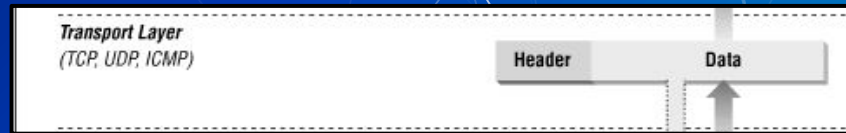


Intro to Ports

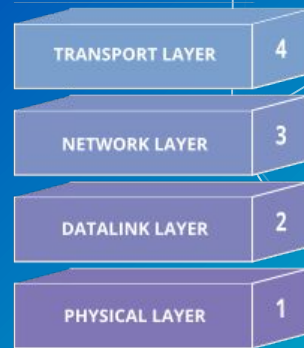
- Ports are similar to room numbers
 - MAC: 43.000483,
-78.783078
 - IP: 103 Center for the Arts
 - Port: Room 116
- Ports are indicated next to IP addresses
 - 192.168.15.152:**116**



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

source port number 2 bytes				destination port number 2 bytes			
sequence number 4 bytes							
acknowledgement number 4 bytes							
data offset 4 bits		reserved 3 bits		control flags 9 bits		window size 2 bytes	
checksum 2 bytes				urgent pointer 2 bytes			
optional data 0-40 bytes							

UDP Header

Source port	Destination port
UDP length	Checksum

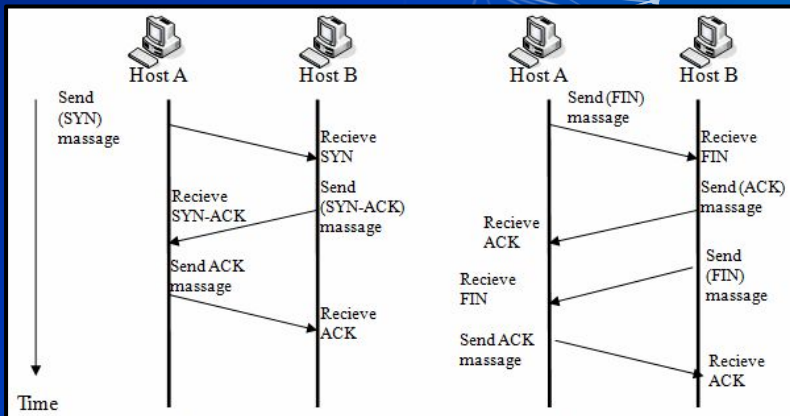
In Class Activity

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

"Application Layer"



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

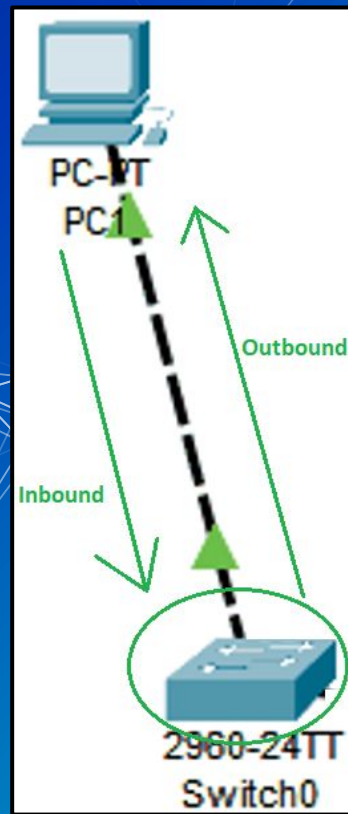
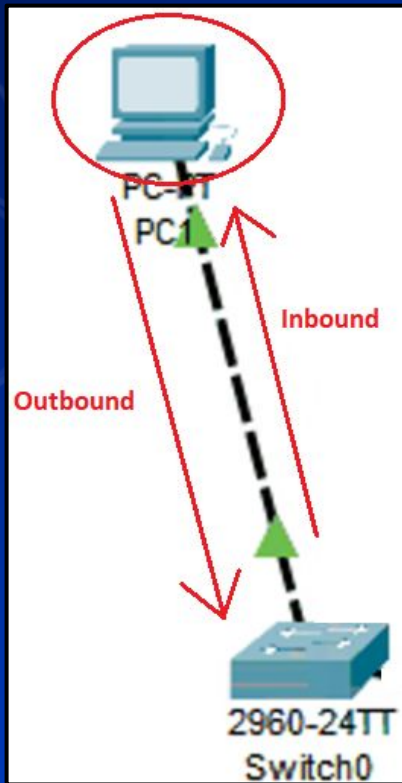
```
Name: google.com
Addresses: 2607:f8b0:4006:81c::200e
          142.250.176.206
```

DNS Demo

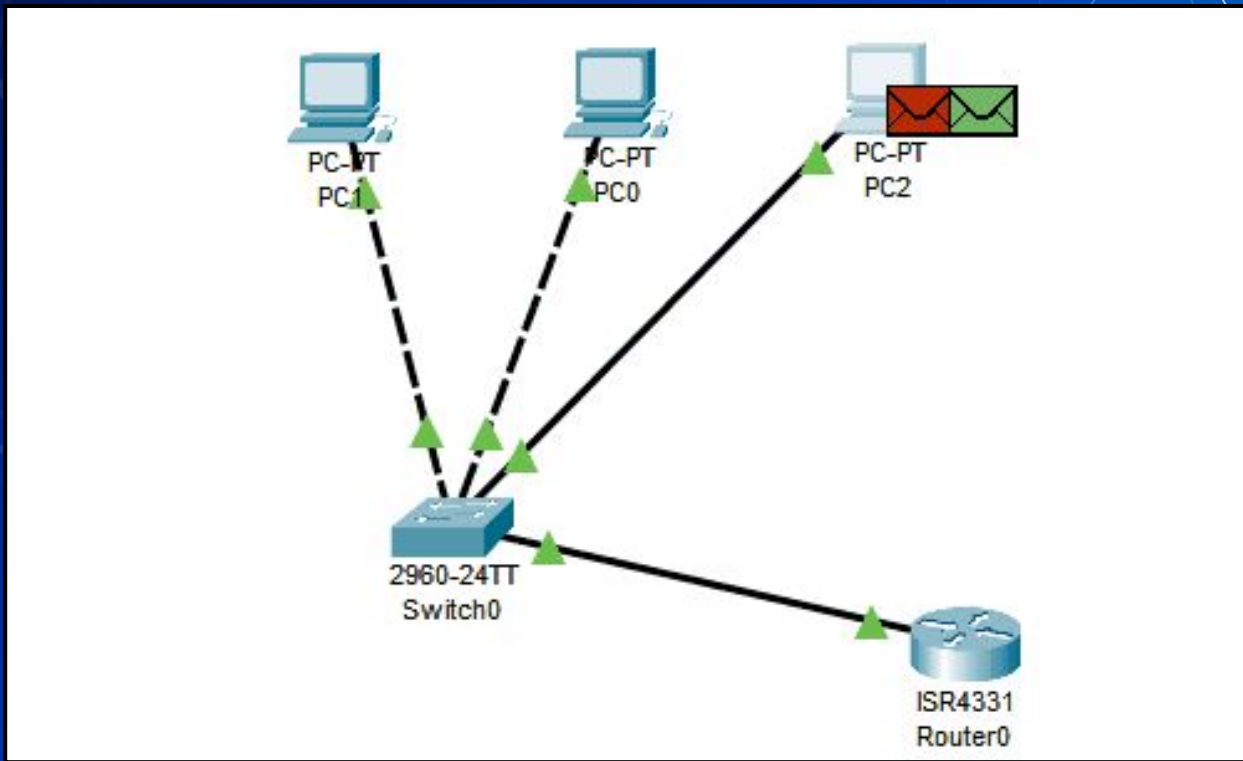
- ⬡ Open a CLI
- ⬡ `nslookup washington.edu`
- ⬡ Copy IP Address into web browser
- ⬡ You may need to use `http://` as a URL prefix

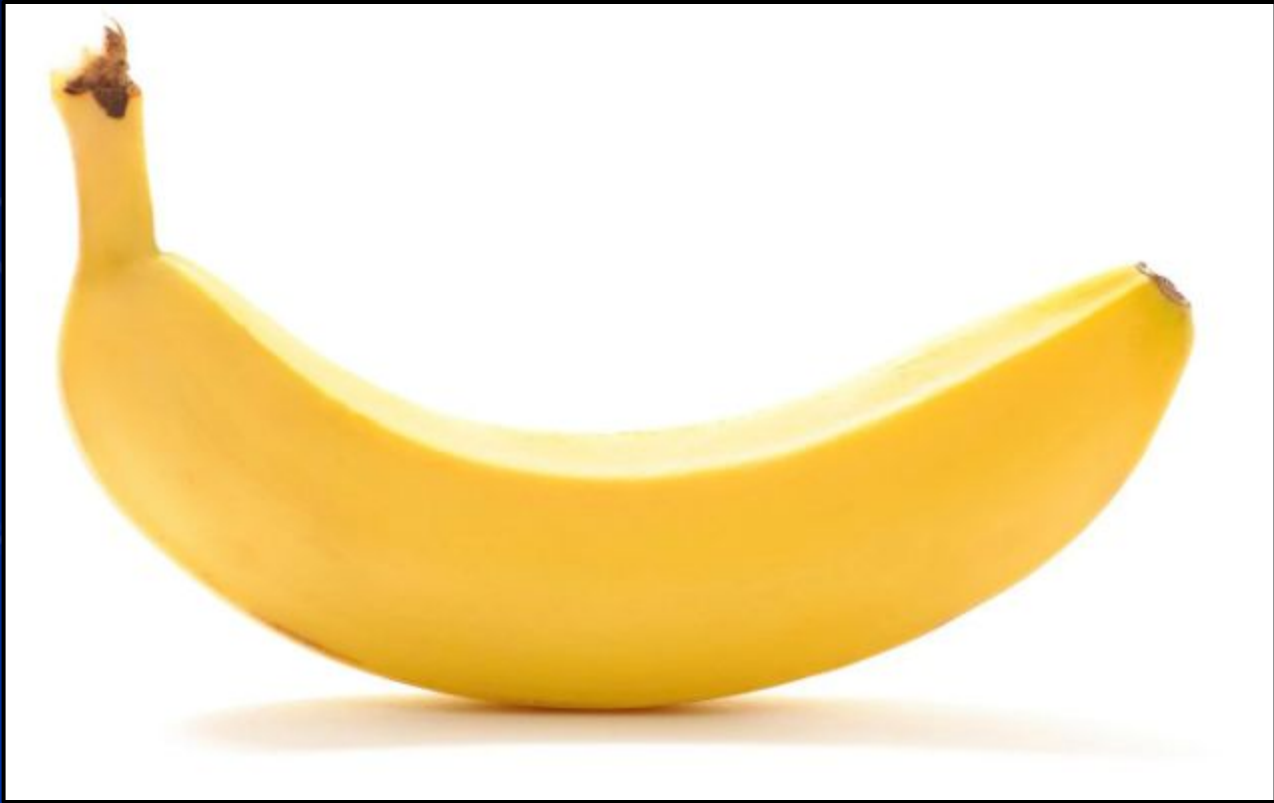


Directional Flow



Data flows freely... for now





Questions?

In Class Activity

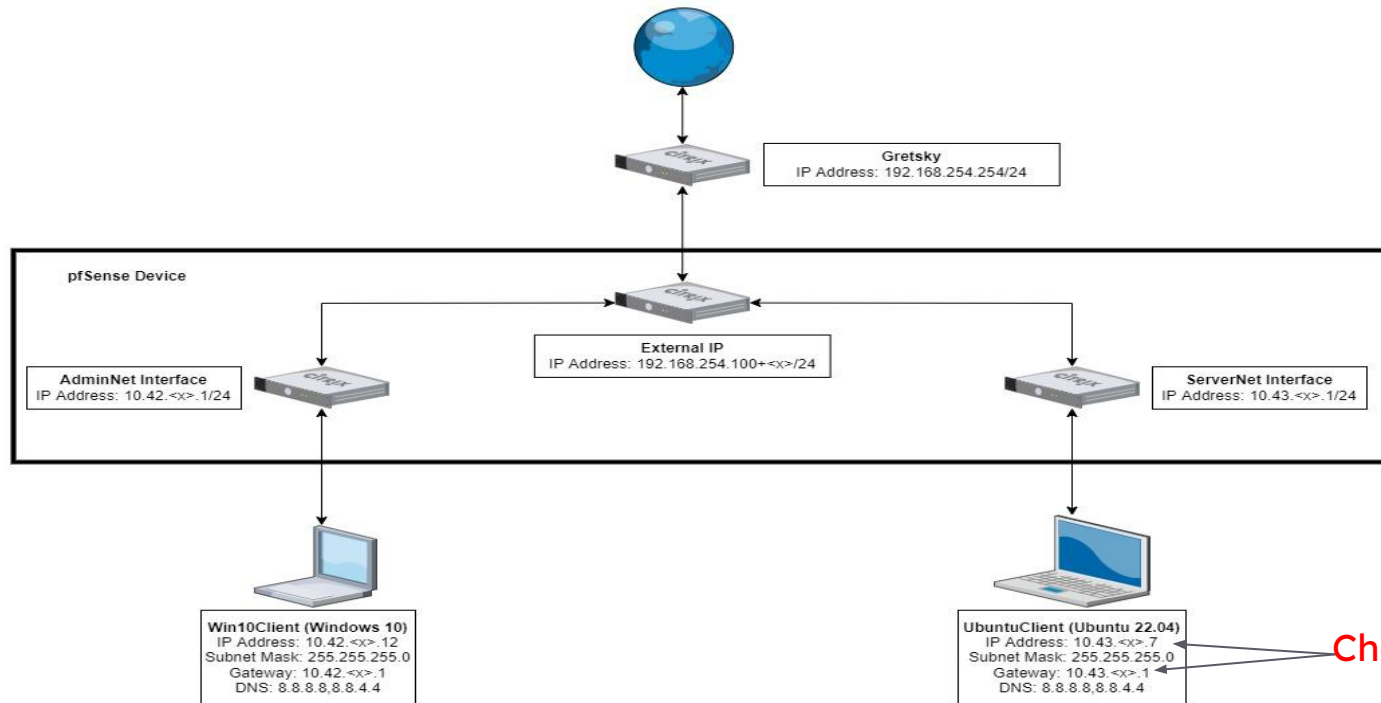
Hands-on Migration

Activity – Migrate Linux to AdminNet

- ⬡ Migrate UbuntuClient from [ServerNet](#) to [AdminNet](#).

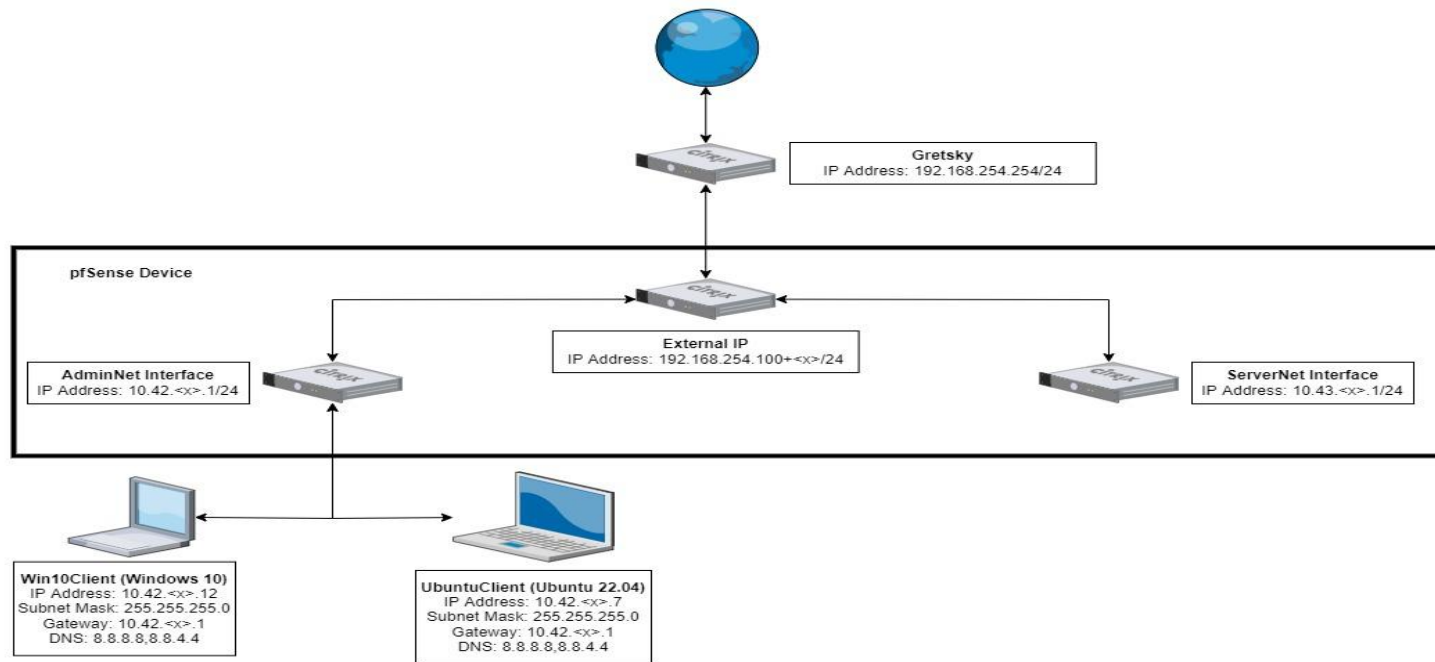
Activity – Migrate Linux to AdminNet

Before

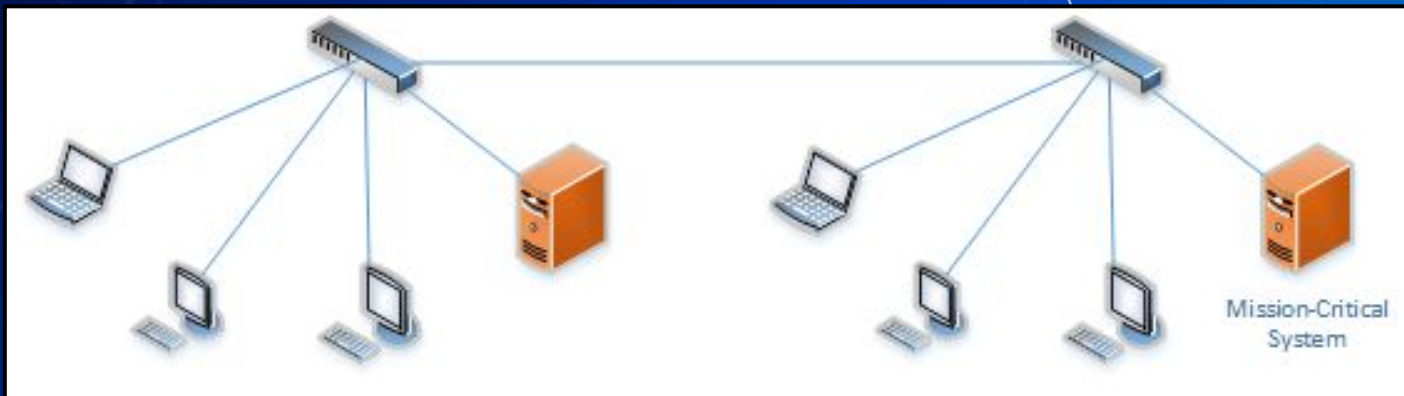


Activity – Migrate Linux to AdminNet

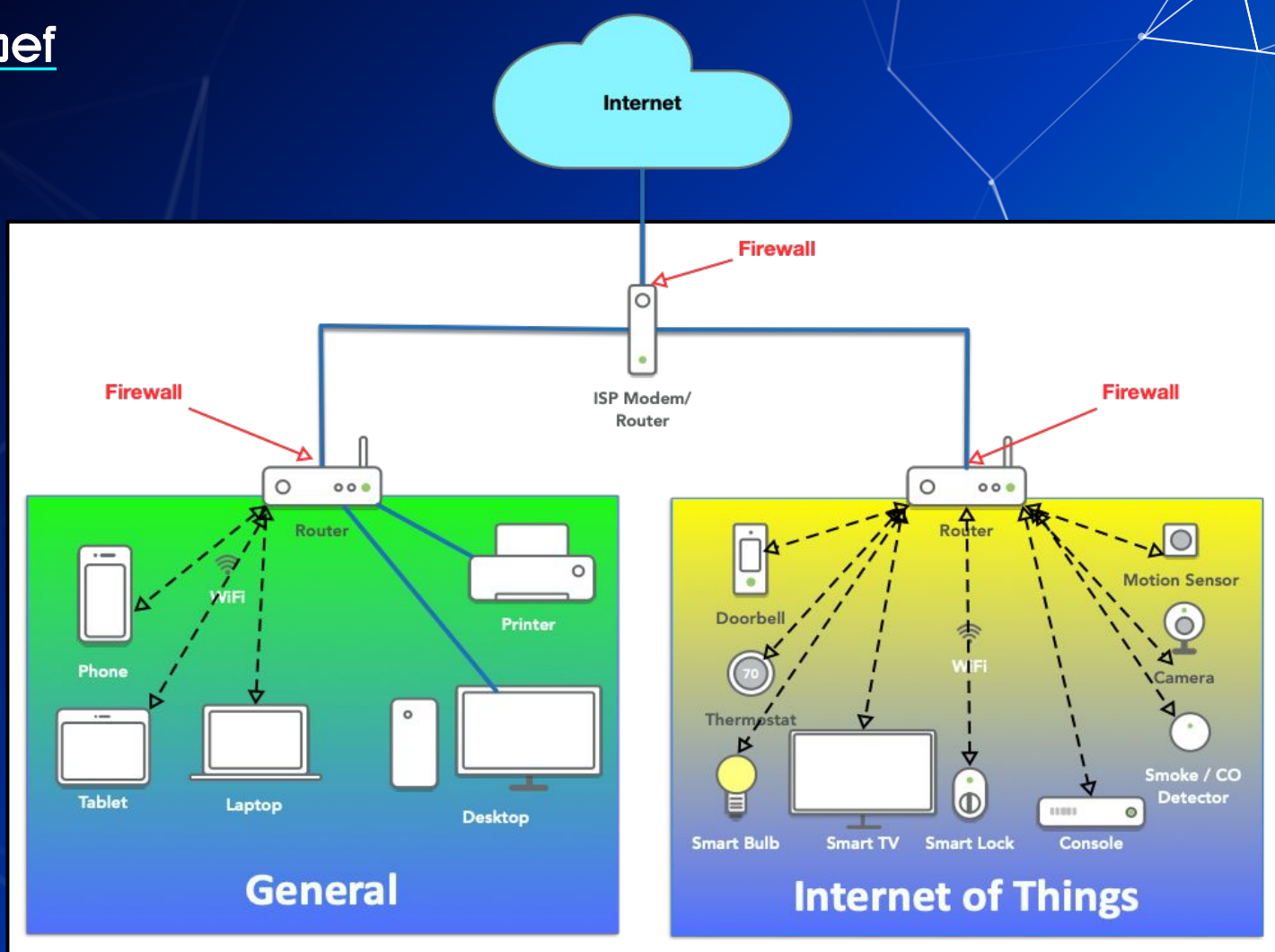
After

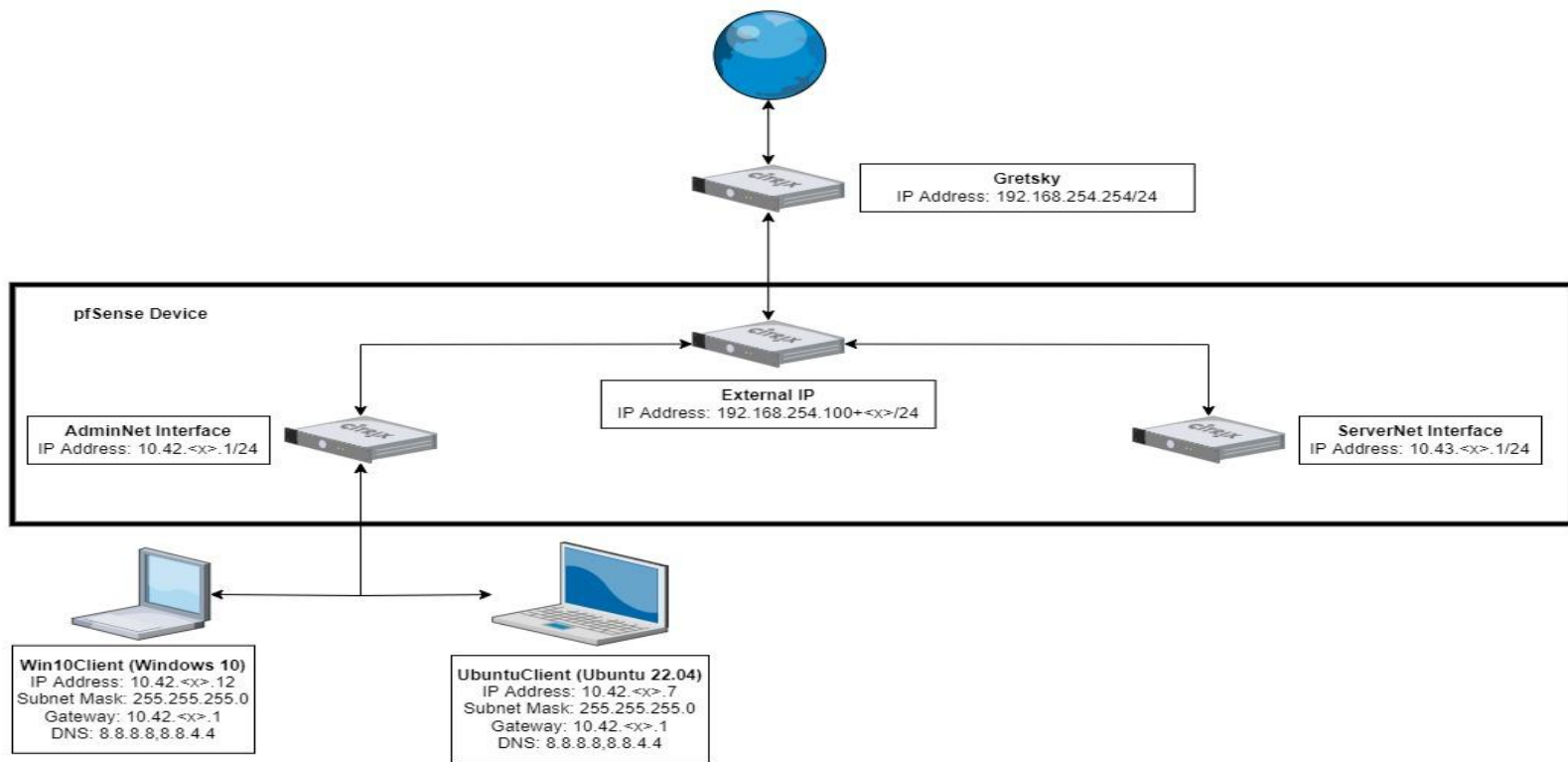


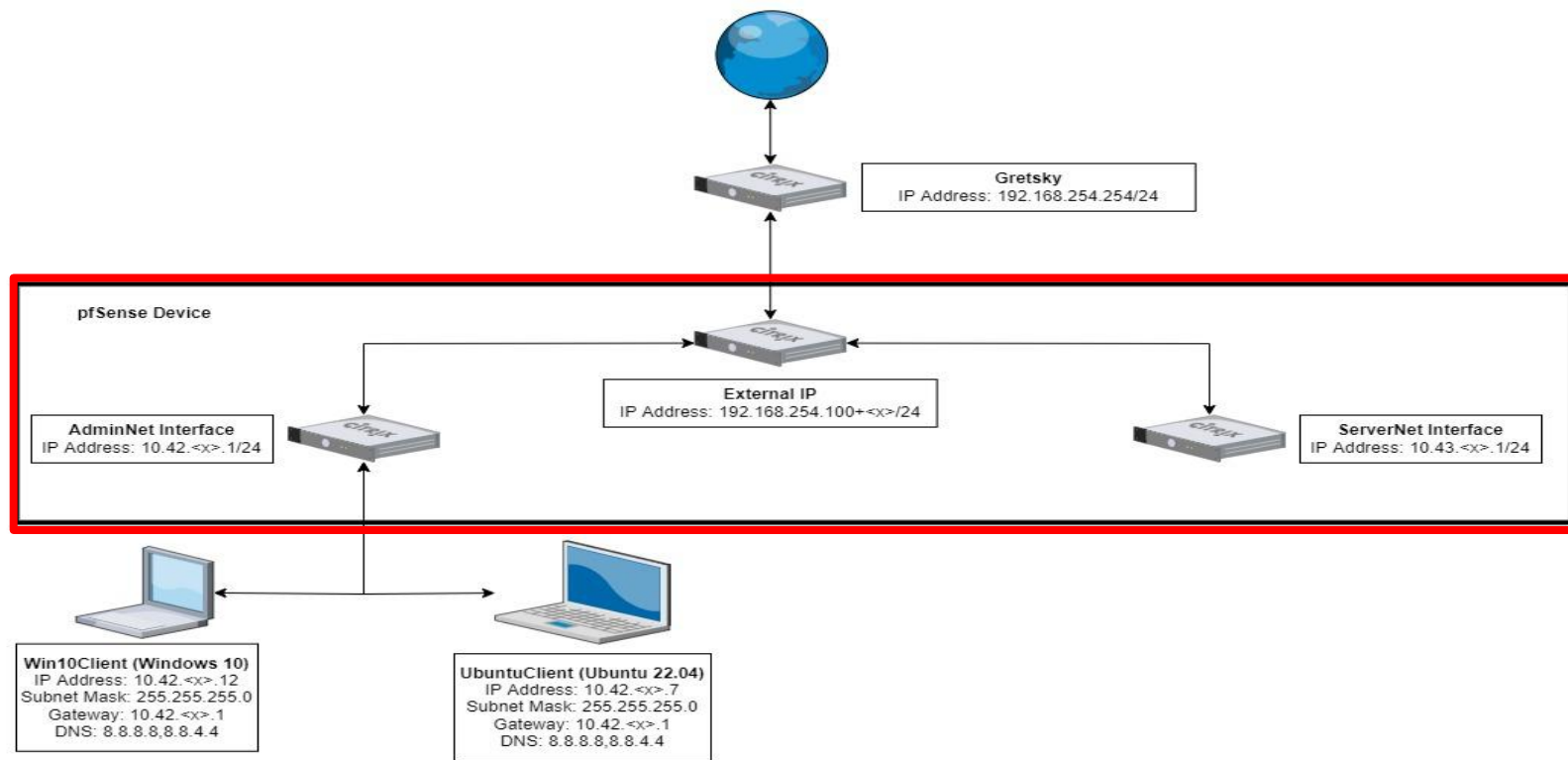
Why Firewalls?

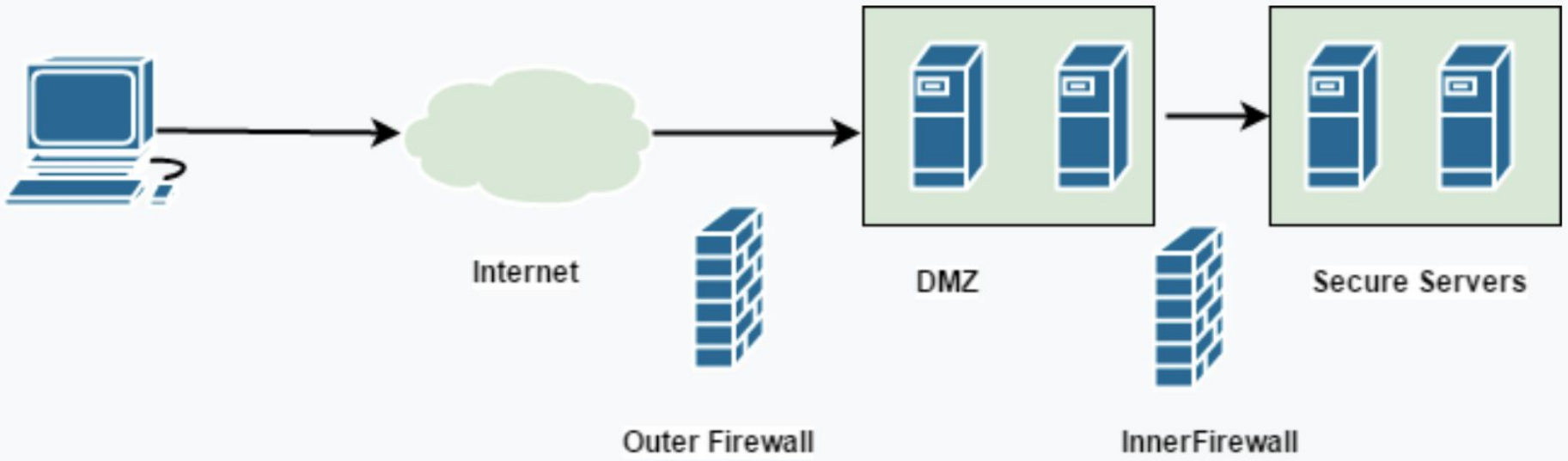


**Any networked device can
access the mission-critical
system**









DMZ

Types of Firewalls

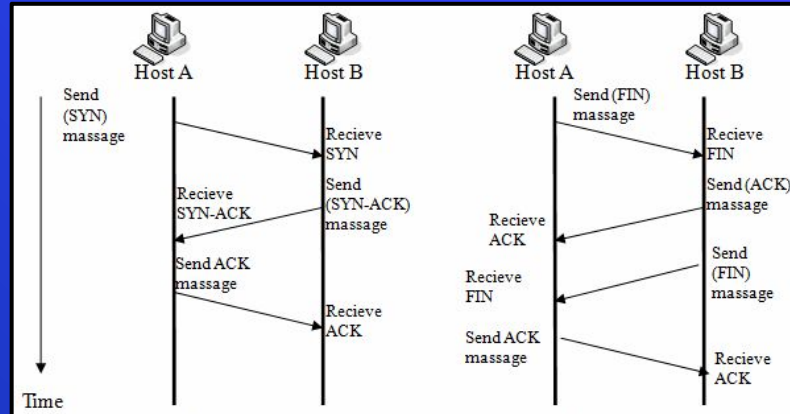
- Packet Filters (GEN 1)
- Stateful Firewalls (GEN 2)
 - Host-Based
 - pfSense
- Next-generation Firewalls (NGFW)
 - Palo Alto (coming soon in this class)

In Class Activity

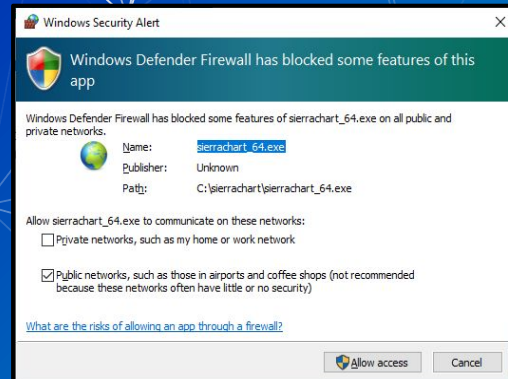
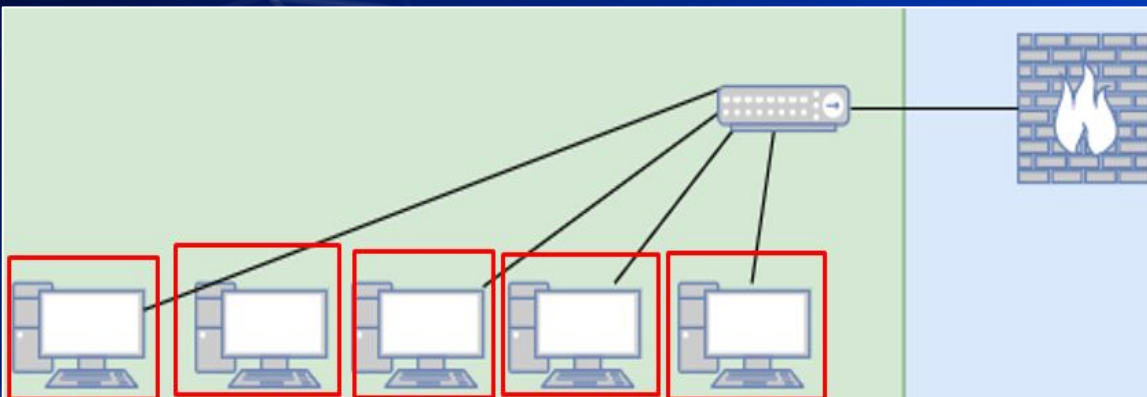
TCP/UDP Packet Polo with Firewall



TCP/UDP Packet Polo with Firewall



Host based Firewalls



```
root@nixcraft:~# iptables -A INPUT -s 202.54.1.1 -j DROP -m comment --comment "DROP spam IP address"
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    tcp  --  0.0.0.0/0             0.0.0.0/0          tcp dpt:53
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0          tcp dpt:67
ACCEPT    udp  --  0.0.0.0/0             0.0.0.0/0          udp 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:~# 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 HTTPS access" -j DROP
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    tcp  --  0.0.0.0/0             0.0.0.0/0          tcp dpt:53
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0          tcp dpt:67
ACCEPT    tcp  --  0.0.0.0/0             0.0.0.0/0          tcp 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 HTTPS access */
```


Break slide

Please return in 10 minutes

Also turn on your Win10Client

In Class Activity



Login to pfSense

Accessing pfSense

- ⬡ Open your 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 dropdown 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

Reserved Networks

Block private networks and loopback addresses ☒ Blocks traffic from IP addresses th RFC 4193 (fc00::7) as well as loop private address space, too.

Block bogon networks ☒ Blocks traffic from reserved IP add routing table, and so should not ap This option should only be used on Note: The update frequency can be

 Save

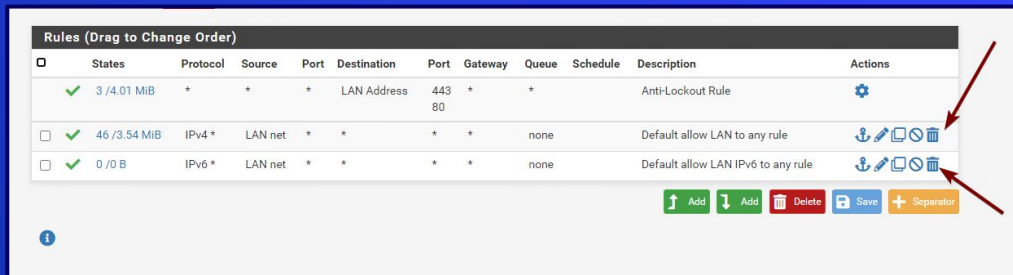
Disabling Default LAN(AdminNet) Firewall Rules (Cont.)



- Change your interface to your LAN (AdminNet)

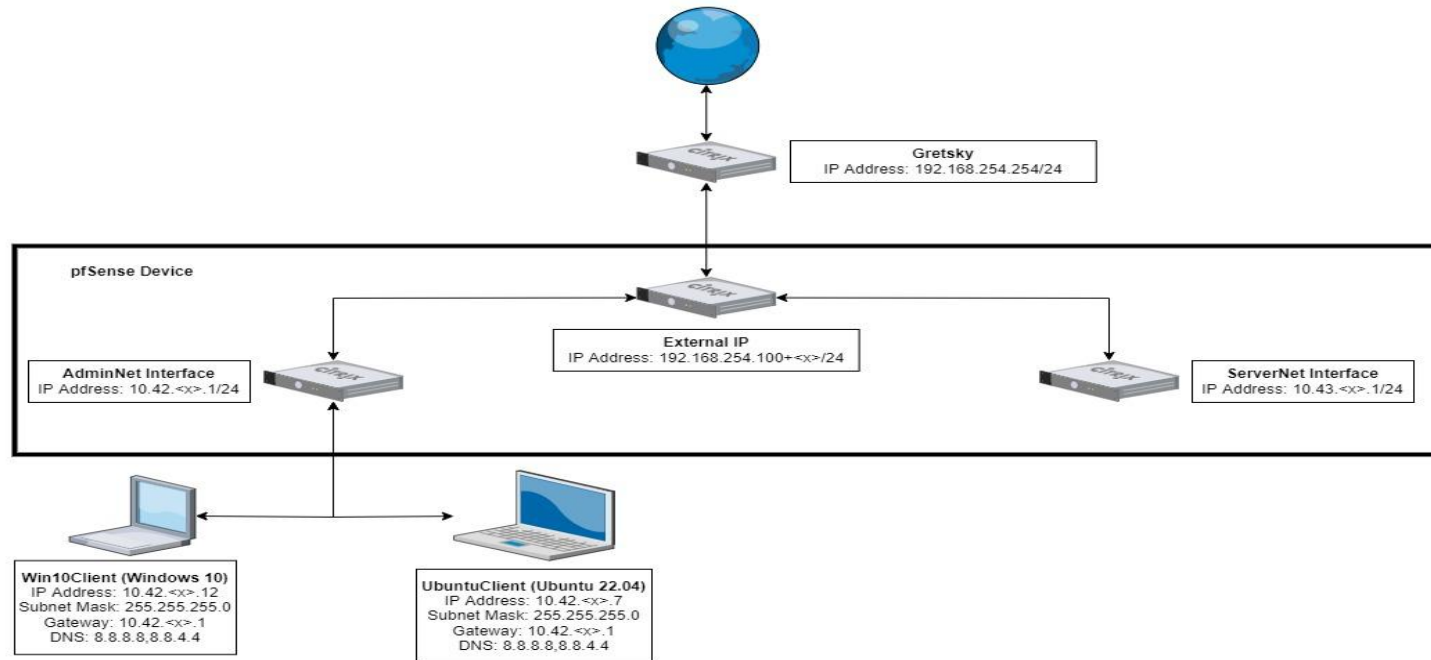


- Remove the default firewall rules, remember to save and apply after
















- Do not** remove the Anti-Lockout Rule... yet! (Hint: that's part of your HW)

Current Network State



Header to Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP <i>any</i>	*	*	8.8.8.8	*	*	none			    
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			    
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			    
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			    

Packet Header

Protocol







Source IP Addr

Destination IP Addr

source port number
2 bytes

destination port number
2 bytes

Header to Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			    
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			    
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			    
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			    

Packet Header

Protocol




















Source IP Addr

Destination IP Addr

source port number
2 bytes

destination port number
2 bytes

Header to Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP <u>any</u>	*	*	8.8.8.8	*	*	none			    
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			    
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			    
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			    

Packet Header

Protocol










Source IP Addr

Destination IP Addr

source port number
2 bytes

destination port number
2 bytes

Header to Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP any.	*	*	8.8.8.8	*	*	none			   
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			   
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			   
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			   

Packet Header

Protocol

















Source IP Addr

Destination IP Addr

source port number
2 bytes

destination port number
2 bytes

Header to Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			   
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			   
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			   
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			   

Packet Header

Protocol

Source IP Addr

Destination IP Addr

source port number
2 bytes

destination port number
2 bytes

Header to Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			

Packet Header

Protocol

Source IP Addr

Destination IP Addr

source port number
2 bytes

destination port number
2 bytes

The Logic of Firewalls

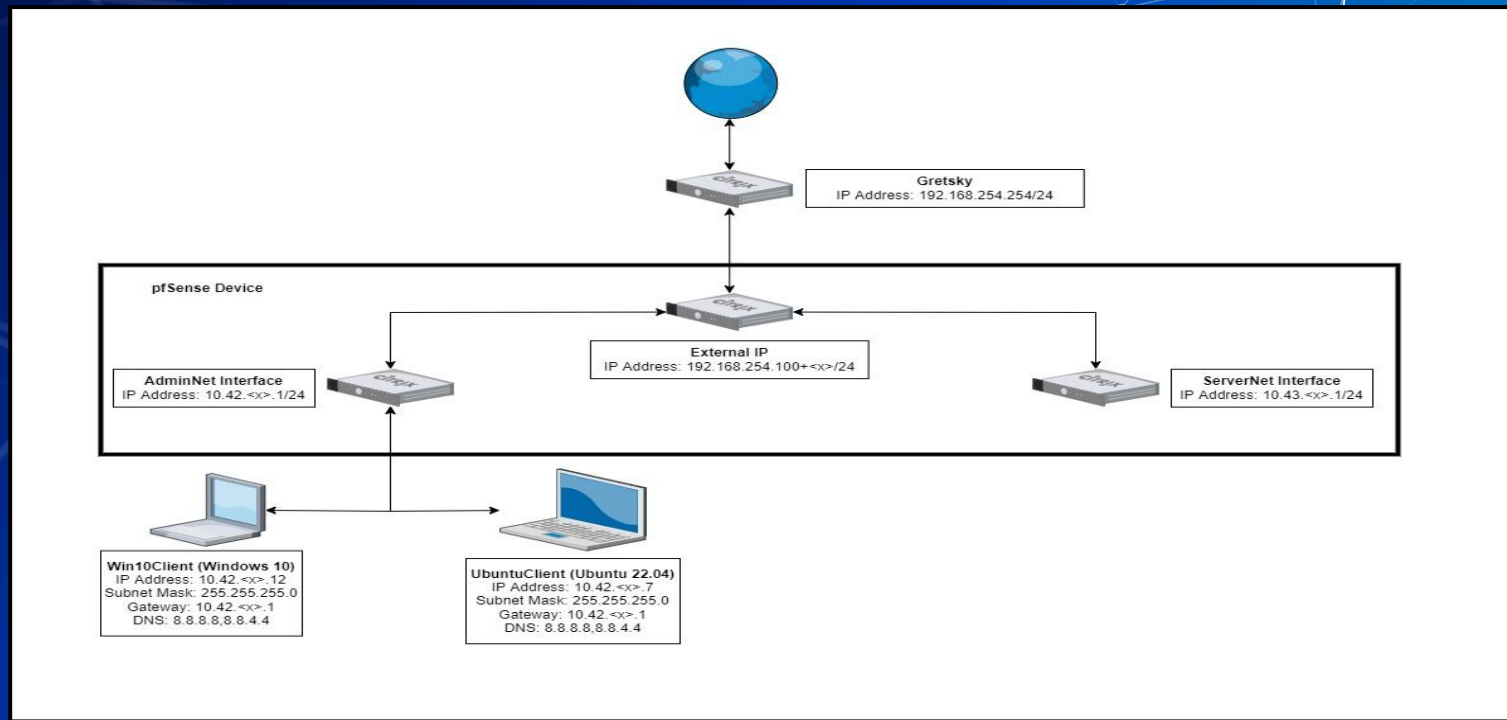
Rule Hierarchy

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

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /480 B	IPv4 ICMP any.	*	*	8.8.8.8	*	*	none			    
<input type="checkbox"/>	✓ 0 /217 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			    
<input type="checkbox"/>	✓ 0 /877 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			    
<input type="checkbox"/>	✗ 0 /1 KiB	IPv4 TCP	*	*	*	*	*	none			    

How Traffic Flows

■ Your network



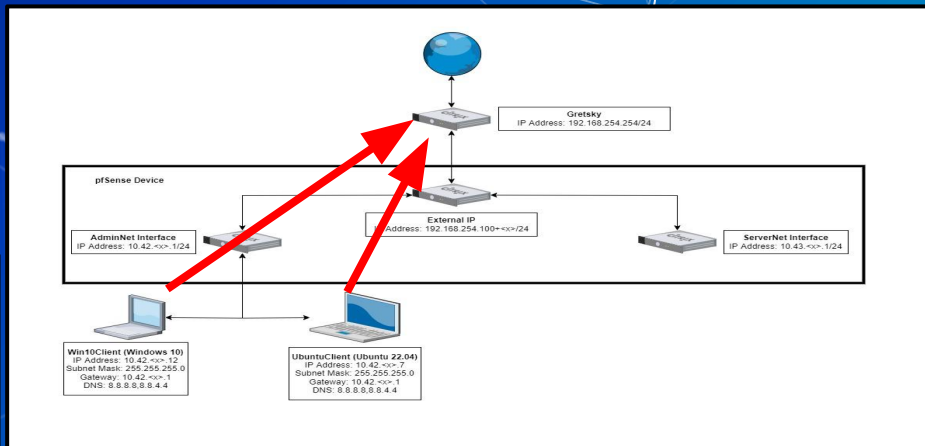
How Traffic Flows

- From LAN (AdminNet) to Web

Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway
<input type="checkbox"/>	✓ 0 / 480 B	IPv4 ICMP <u>any</u>	*	*	8.8.8.8	*	*



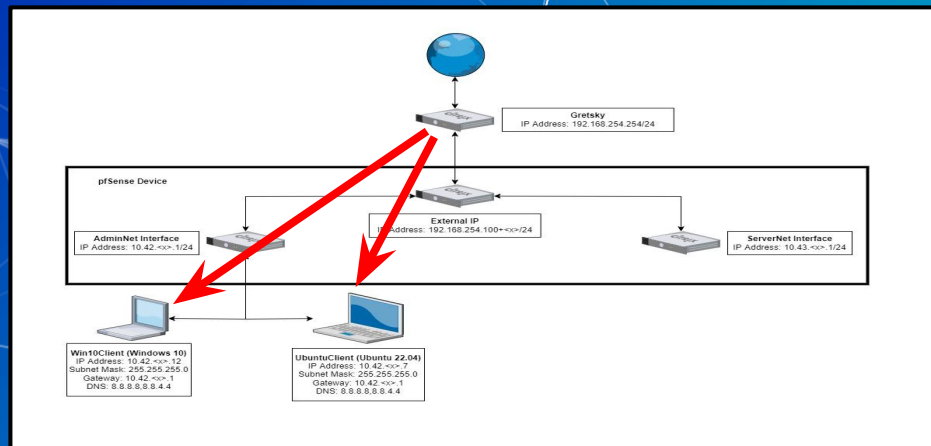
How Traffic Flows

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

Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway
<input type="checkbox"/>	✓ 2/249 KiB	IPv4 TCP	192.168.13.71	*	10.42.29.11	3389	*



Catch all rule

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

Catch all 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)

- Default firewall rule(s) need to be at the bottom of the firewall's rule list

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?

In Class Activity

Compromised Device & pfSense Hands-On

Activity – pfSense Firewall

- Prevent all ping requests from inside **AdminNet** to anywhere on **External** (Anywhere on Gretzky's LAN or the internet)
 - Test by attempting to ping IP address 8.8.8.8
- If this is too easy
 - Make it so you can ping Gretzky (192.168.254.254) but not 8.8.8.8

Activity – Compromised Windows 10 Host

- Prevent me from being able to access your system.
 - Credentials:
 - Username: sysadmin
 - Password: Change.me!
- Hint[0]: get-nettcpconnection
- Hint[1]: What are the remote control protocols that Windows uses?

Homework Prep

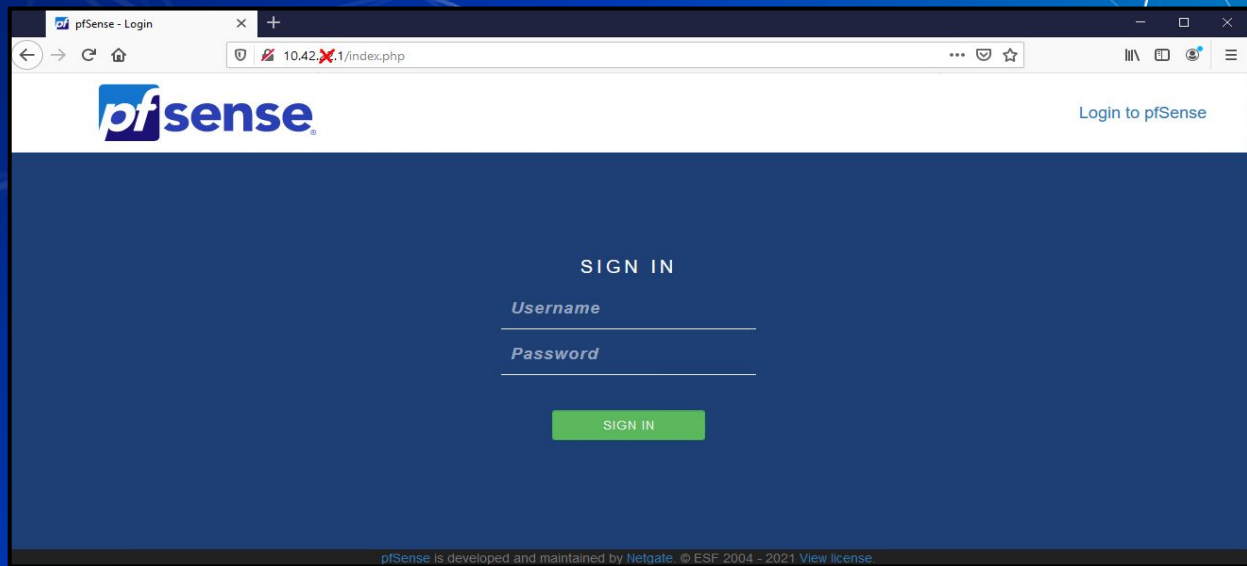
System Prep

- 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=Z6kNyfZiNyg>

Homework Starter

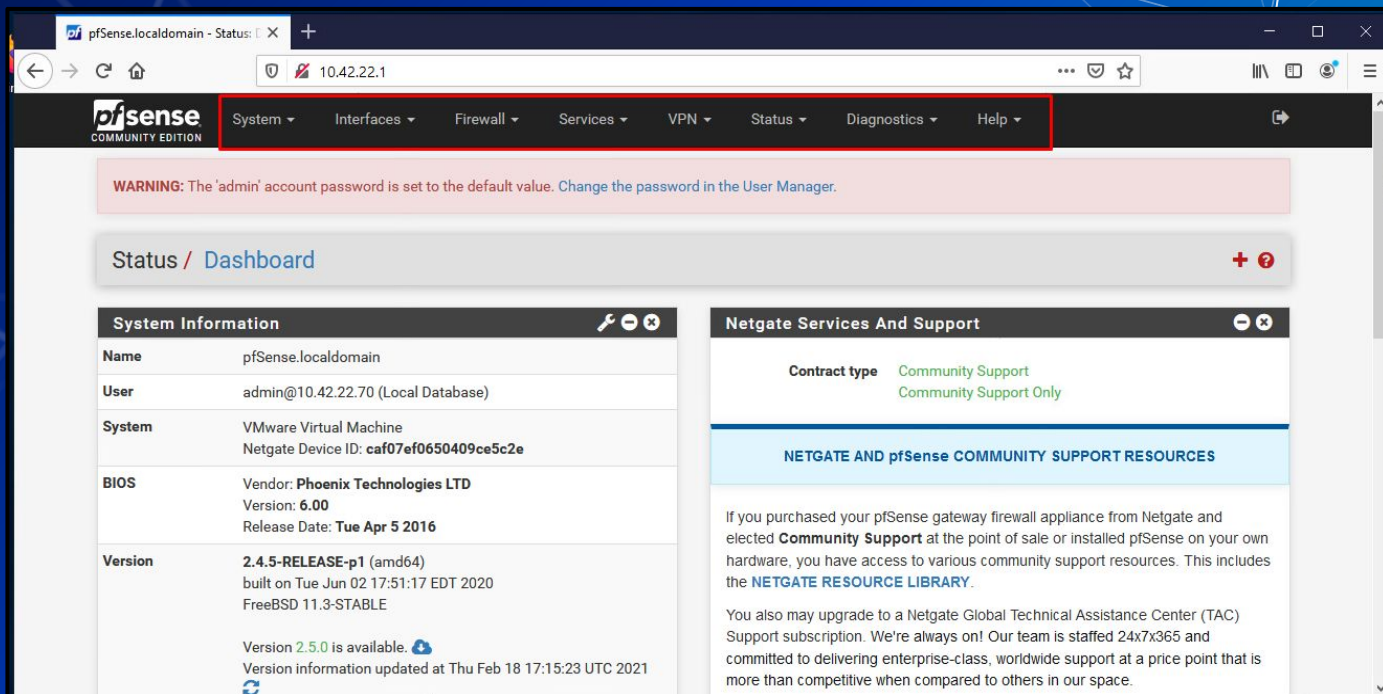
Homework Starter

- Credentials
 - Username: admin
 - Password: pfsense



Homework Starter

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



pfSense.localdomain - Status: 10.42.22.1

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

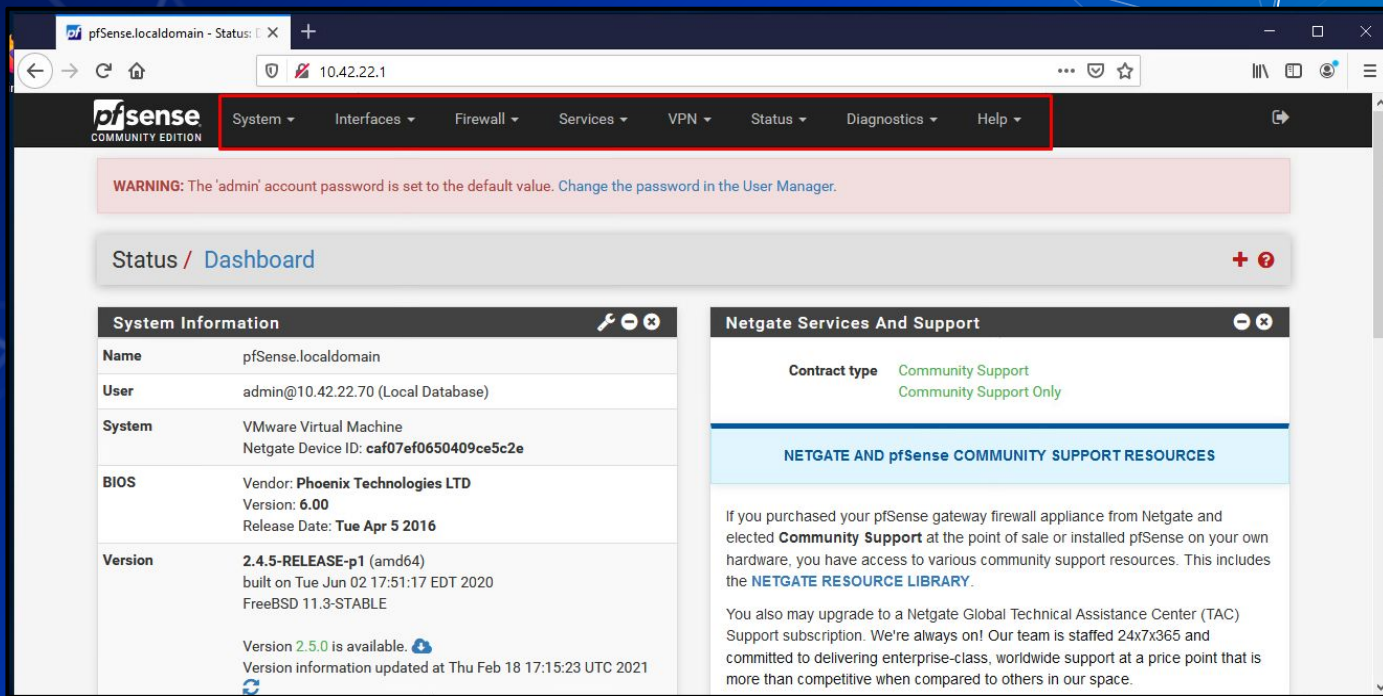
Status / Dashboard

System Information	
Name	pfSense.localdomain
User	admin@10.42.22.70 (Local Database)
System	VMware Virtual Machine Netgate Device ID: caf07ef0650409ce5c2e
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Tue Apr 5 2016
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE Version 2.5.0 is available. View details Version information updated at Thu Feb 18 17:15:23 UTC 2021

Netgate Services And Support	
Contract type	Community Support Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES	
<p>If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.</p> <p>You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.</p>	

Homework Starter

- Rules menu is under Firewall > Rules



The screenshot shows the pfSense web interface. The top navigation bar includes the pfSense logo and a menu with the following items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'Firewall' menu item is highlighted with a red box. Below the navigation bar, a warning message states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main content area is titled 'Status / Dashboard' and contains two panels. The left panel, 'System Information', displays details about the pfSense instance, including the name, user, system type, BIOS version, and the current pfSense version (2.4.5-RELEASE-p1). The right panel, 'Netgate Services And Support', shows the contract type as 'Community Support' and provides links to 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' and 'NETGATE RESOURCE LIBRARY'.

pfSense.localdomain - Status | 10.42.22.1

pfSense COMMUNITY EDITION

System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@10.42.22.70 (Local Database)
System	VMware Virtual Machine Netgate Device ID: caf07ef0650409ce5c2e
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Tue Apr 5 2016
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE Version 2.5.0 is available. View details Version information updated at Thu Feb 18 17:15:23 UTC 2021

Netgate Services And Support

Contract type **Community Support**
Community Support Only

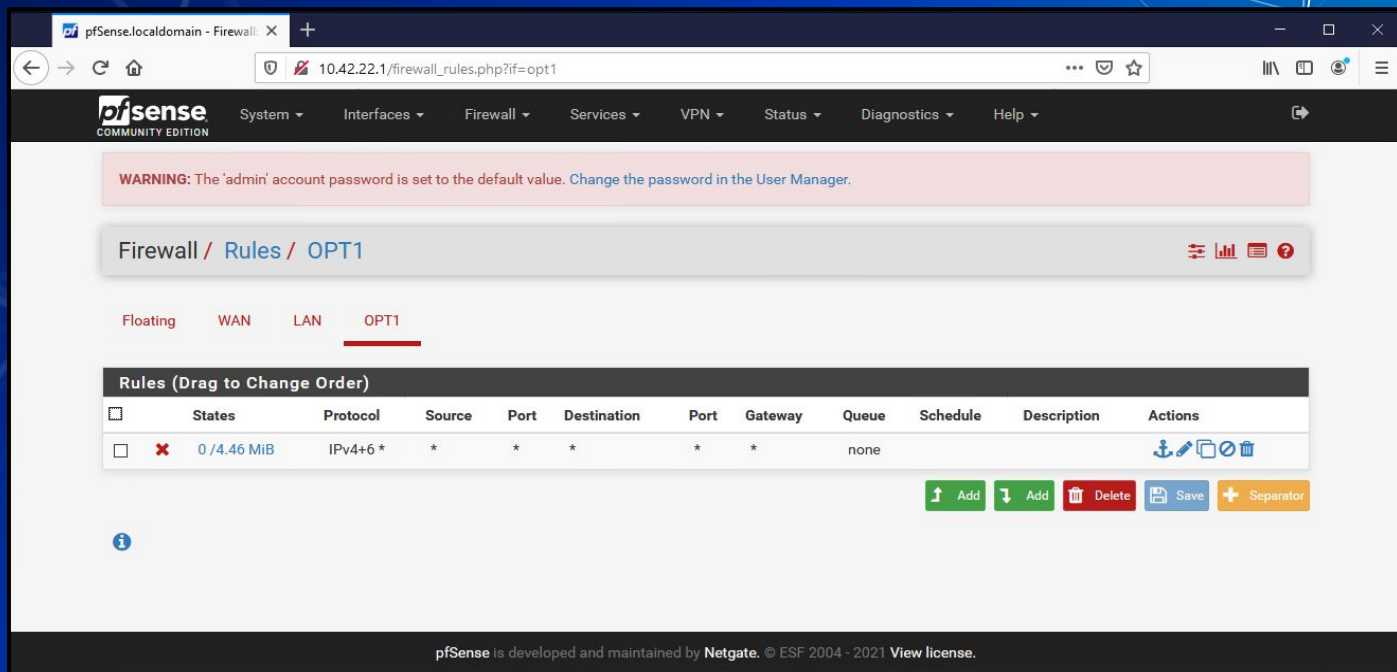
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).






You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

Homework Starter

- Rules are grouped by the interface that handles the packets



The screenshot shows the pfSense web interface for configuring Firewall Rules. The browser address bar shows the URL `10.42.22.1/firewall_rules.php?if=opt1`. The page title is "Firewall / Rules / OPT1". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the warning, the "OPT1" tab is selected under the "Rules (Drag to Change Order)" section. The table below shows the current rule configuration:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 0/4.46 MiB	IPv4+6 *	*	*	*	*	*	none			   

At the bottom of the table, there are buttons for "Add", "Add", "Delete", "Save", and "Separator".

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

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 any 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 Question

Class dismissed

See you next week!