Firewalls

UBNetDef, Fall 2021
Week 3

Lead Presenter:
Anthony Magrene

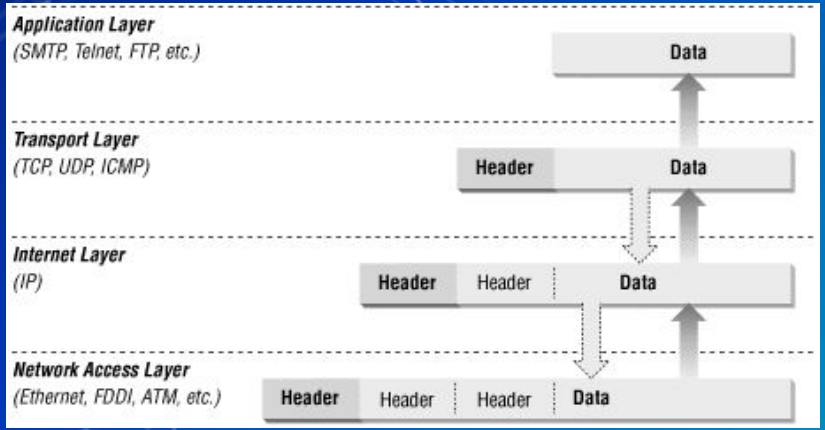
Agenda – Week 3

- Networking Recap
- Why Firewalls?
- Hands-on Activity 1
- The Logic of Firewalls
- Hands-on Activity 2
- Hands-on Activity 3-4
- Homework System Prep

Networking Recap

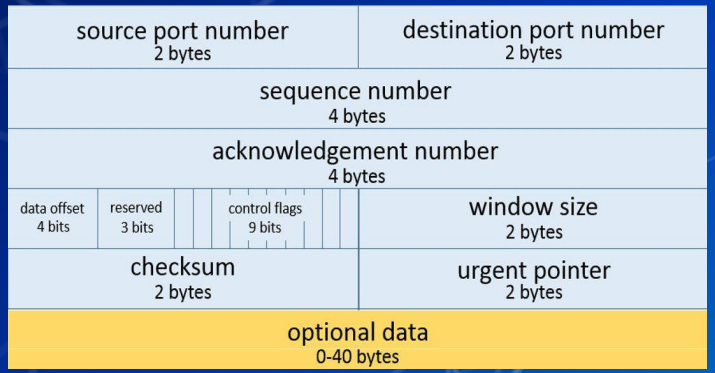
Networking Recap

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



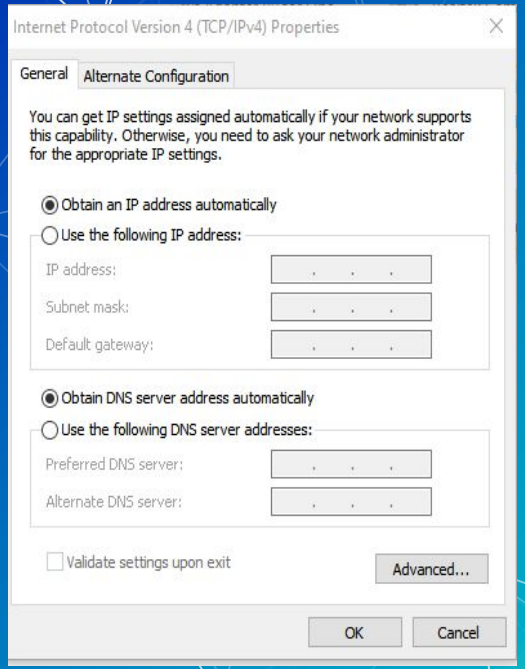
Networking Recap

- TCP has sessions
- UDP does not have sessions



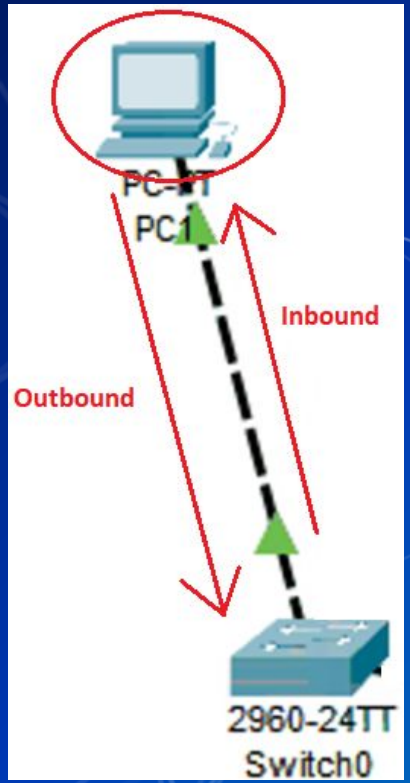
Networking Recap

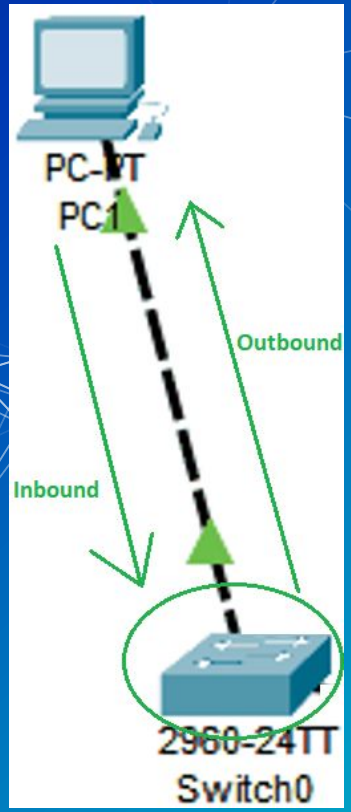
- IP Addresses contain 4 octets 0-255.0-255.0-255.0-255
  - 0 reserved
  - 255 used to the broadcast address
- Subnet masks let us separate IP addresses
  - We can create Local Area Networks (LAN)
- Default gateway is where data must go to leave our LAN
- Domain Name Service makes life easy for us but is not required



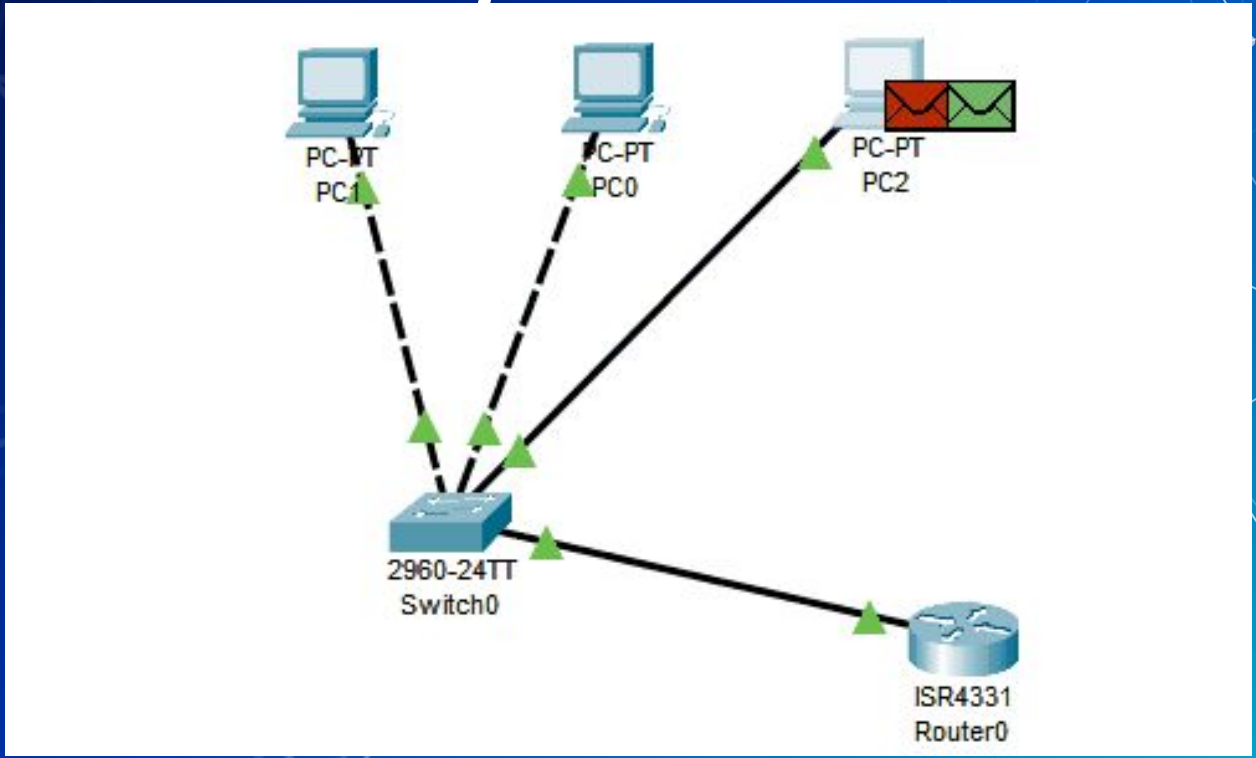

```
PS C:\Users\AnthonyM> resolve-dnsname www.google.com | select Name ,spacer ,IPAddress

Name           spacer IPAddress
----           ------ ---------
www.google.com        2607:f8b0:4006:804::2004
www.google.com        172.217.10.68
```

Directional Flow





Data flows freely... for now



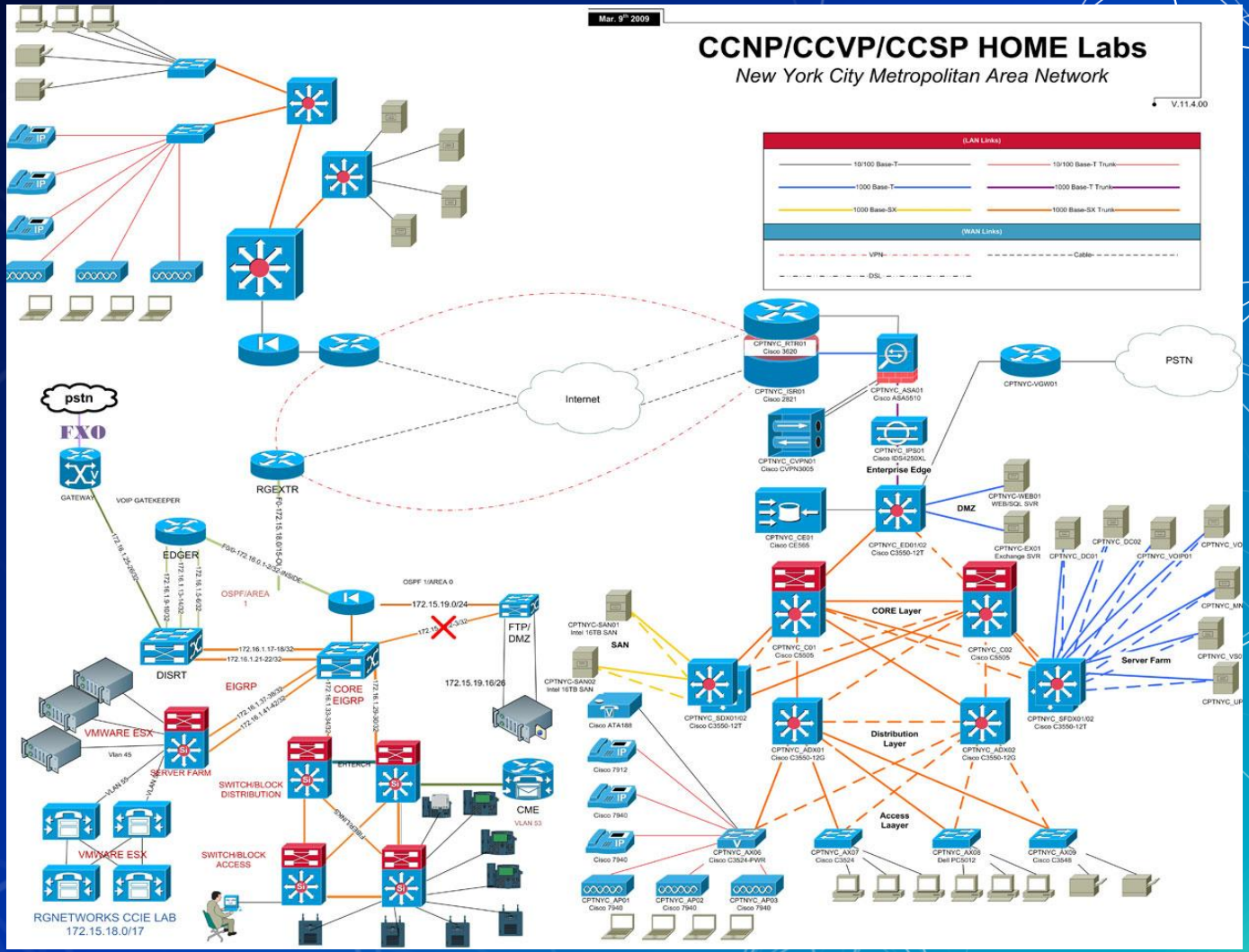
Networking Recap Questions?

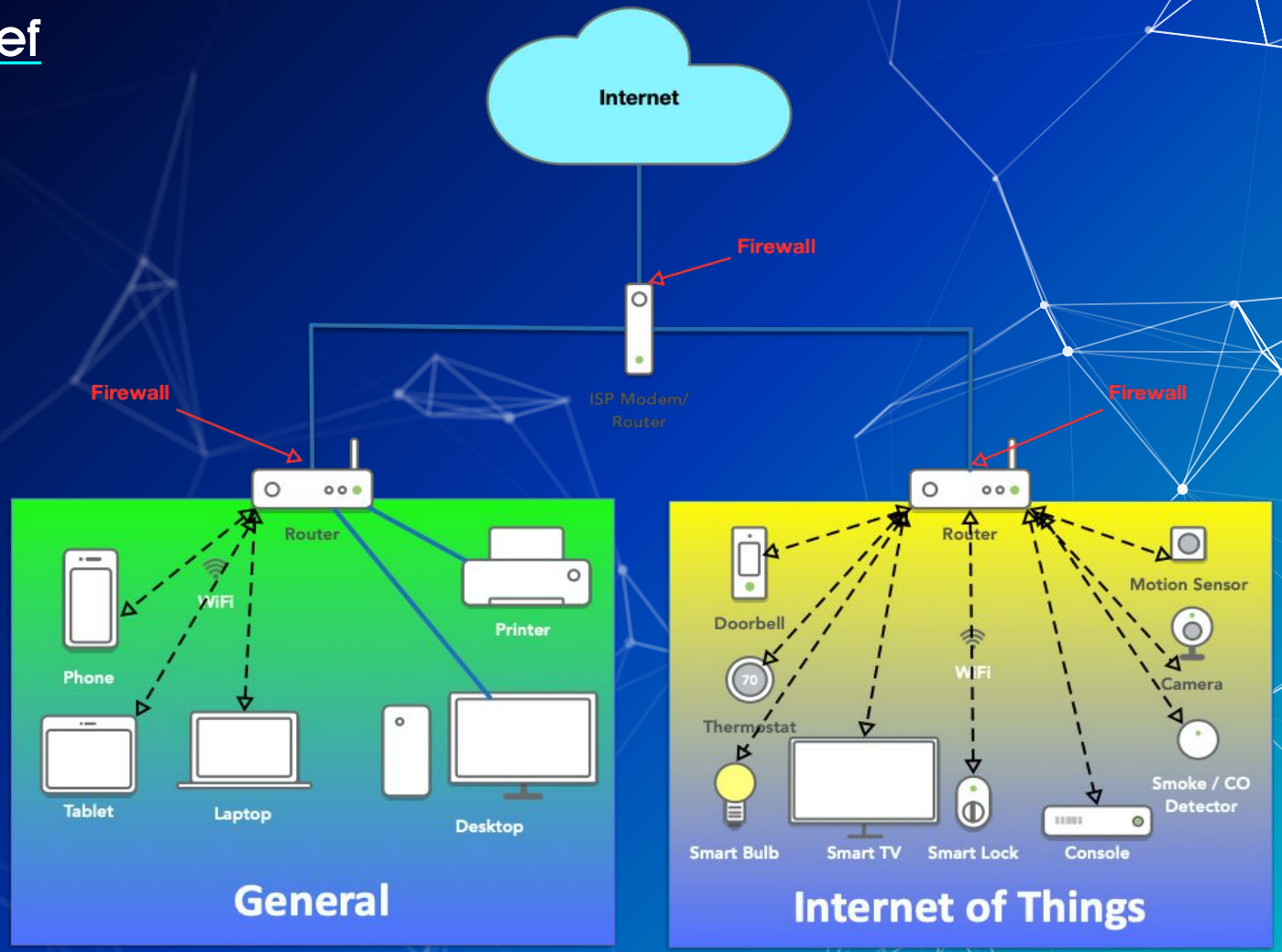
Hands-on Migration

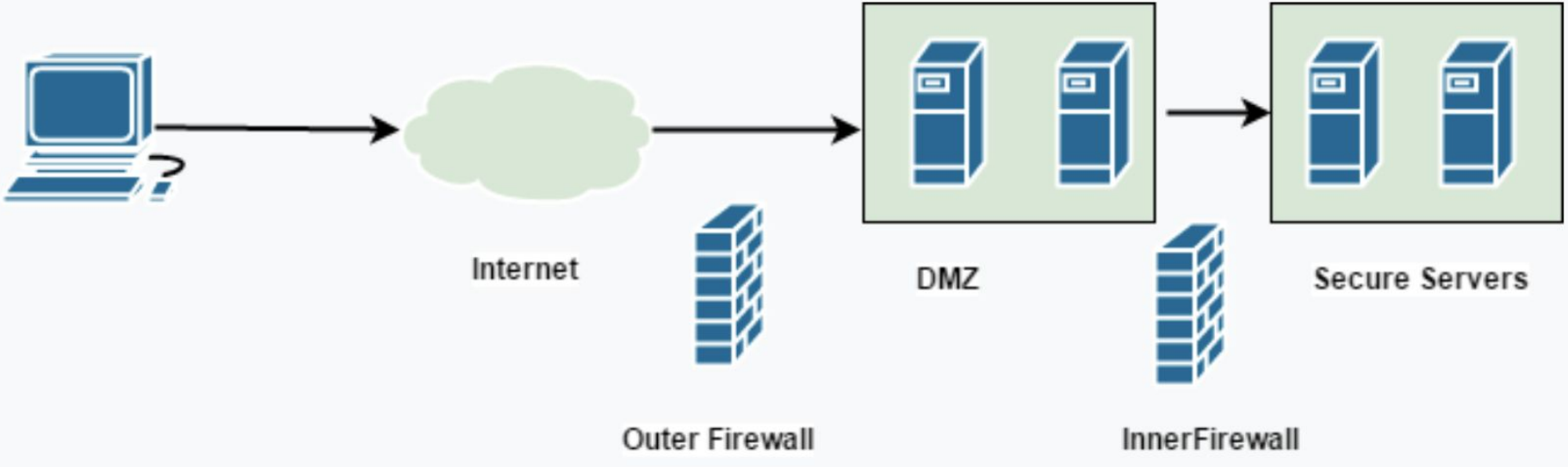
Activity – Migrate Windows to Lan

- Migrate your Windows client from your DMZ to the LAN network

Why Firewalls?


Mar. 9th 2009
CCNP/CCVP/CCSP HOME Labs
New York City Metropolitan Area Network
V.11.4.00
(LAN Links)
10/100 Base-T
10/100 Base-T Trunk
1000 Base-T
1000 Base-T Trunk
1000 Base-SX
1000 Base-SX Trunk
(WAN Links)
VPN
Cable
DSL
Internet
PSTN
CPTNYC_RTR01 Cisco 3620
CPTNYC_ISR01 Cisco 2821
CPTNYC_ASA01 Cisco ASA5510
CPTNYC-VGW01
CPTNYC_CVPN01 Cisco CVPN3005
CPTNYC_IPS01 Cisco IDS4250XL
Enterprise Edge
CPTNYC_CE01 Cisco CE565
CPTNYC_ED01/02 Cisco C3550-12T
DMZ
CPTNYC-WEB01 WEB/SQL SVR
CPTNYC-EX01 Exchange SVR
CPTNYC_DC01
CPTNYC_DC02
CPTNYC_VOIP01
pstn
FXO
GATEWAY
VOIP GATEKEEPER
RGEXTR
EDGER
OSPF/AREA 1
OSPF 1/AREA 0
172.15.19.0/24
FTP/ DMZ
DISRT
EIGRP
CORE EIGRP
172.15.19.16/26
VMWARE ESX
SERVER FARM
SWITCH/BLOCK DISTRIBUTION
CME
VLAN 53
SWITCH/BLOCK ACCESS
RGNETWORKS CCIE LAB
172.15.18.0/17
CPTNYC-SAN01 Intel 16TB SAN
CPTNYC-SAN02 Intel 16TB SAN
SAN
CPTNYC_C01 Cisco C5505
CPTNYC_C02 Cisco C5505
CORE Layer
CPTNYC_SDX01/02 Cisco C3550-12T
CPTNYC_SFDX01/02 Cisco C3550-12T
Server Farm
CPTNYC_ADX01 Cisco C3550-12G
CPTNYC_ADX02 Cisco C3550-12G
Distribution Layer
Cisco ATA188
Cisco 7912
Cisco 7940
CPTNYC_AX06 Cisco C3524-PWR
CPTNYC_AX07 Cisco C3524
CPTNYC_AX08 Dell PC5012
CPTNYC_AX09 Cisco C3548
Access Laayer
CPTNYC_AP01 Cisco 7940
CPTNYC_AP02 Cisco 7940
CPTNYC_AP03 Cisco 7940


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


Internet
DMZ
Secure Servers
Outer Firewall
InnerFirewall

DMZ

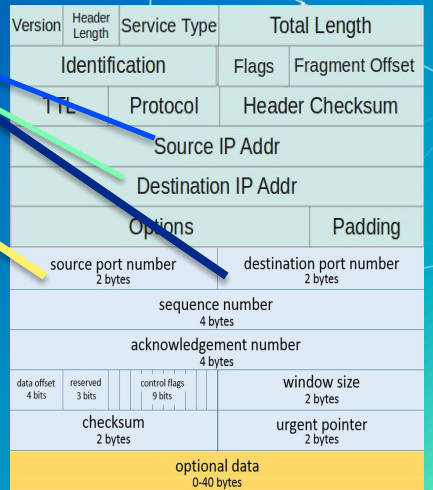
Types of Firewalls

- Packet Filters (GEN 1)
- Stateful Firewalls (GEN 2)
- Next-generation Firewalls (NGFW)
- Host-Based

Packet Filters

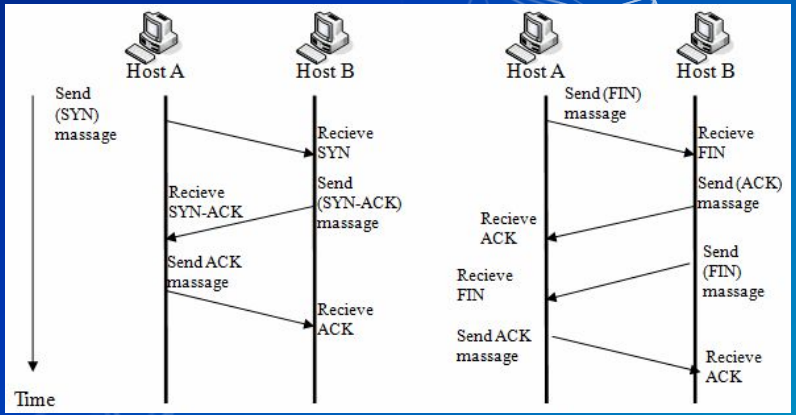
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	1 /2.30 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
☐ ✘	0 /0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		HHTPS Traffic Block	⚓ ✎ ⧉ ⊘ 🗑
☐ ✔	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	⚓ ✎ ⧉ ⊘ 🗑

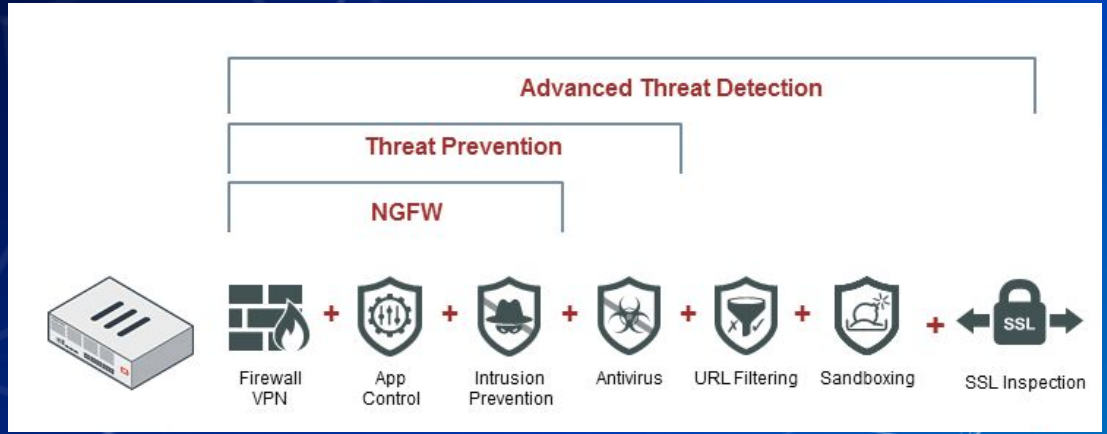


Stateful Firewalls

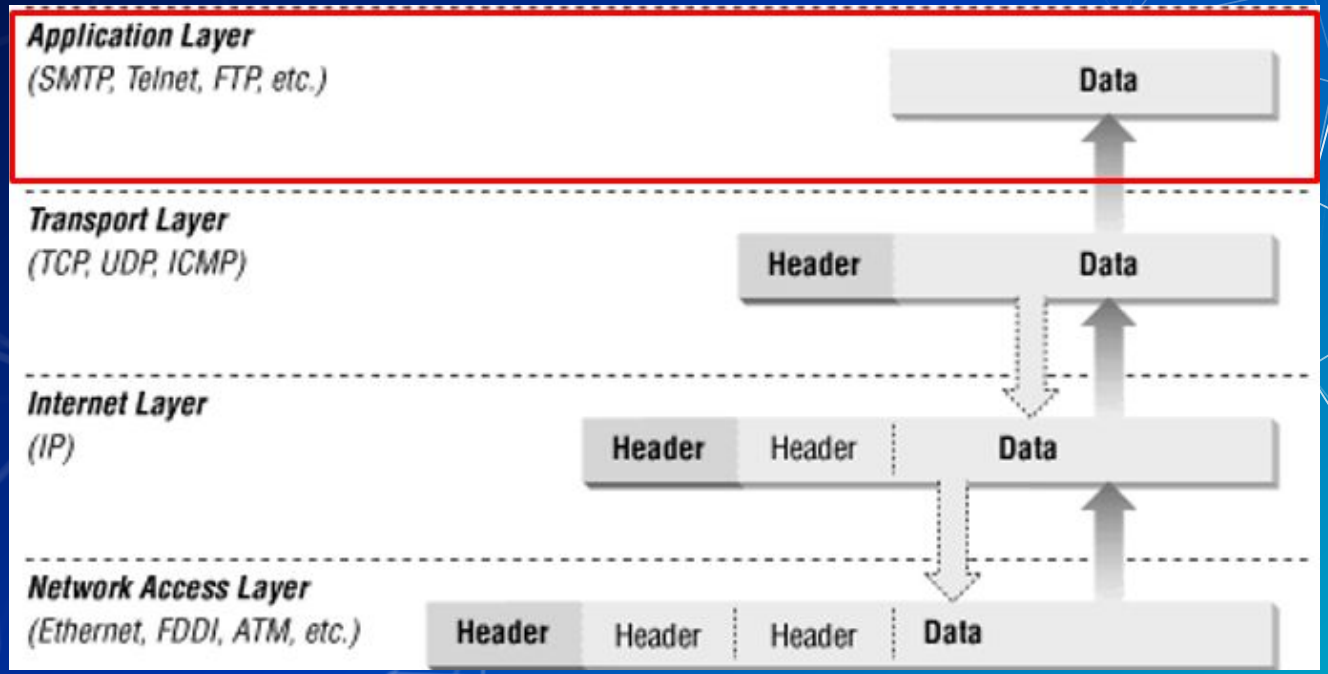
```
pfTop: Up State 1-100/114033, View: default, Order: bytes
PR        DIR SRC                        DEST                        STATE                 AGE       EXP     PKTS    BYTES
icmp      Out 192.168.253.18:17838       192.168.253.17:17838         0:0                75:14:36  00:00:10 1060806 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
```



Next Generation Firewalls

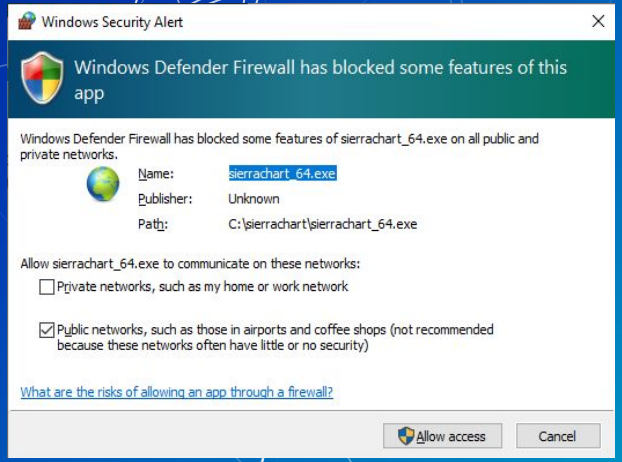


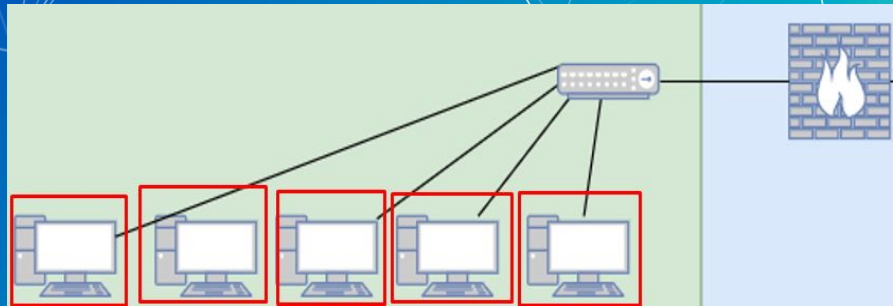
Next Generation Firewalls cont.



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 */
```





Host Based Firewalls Hands-On

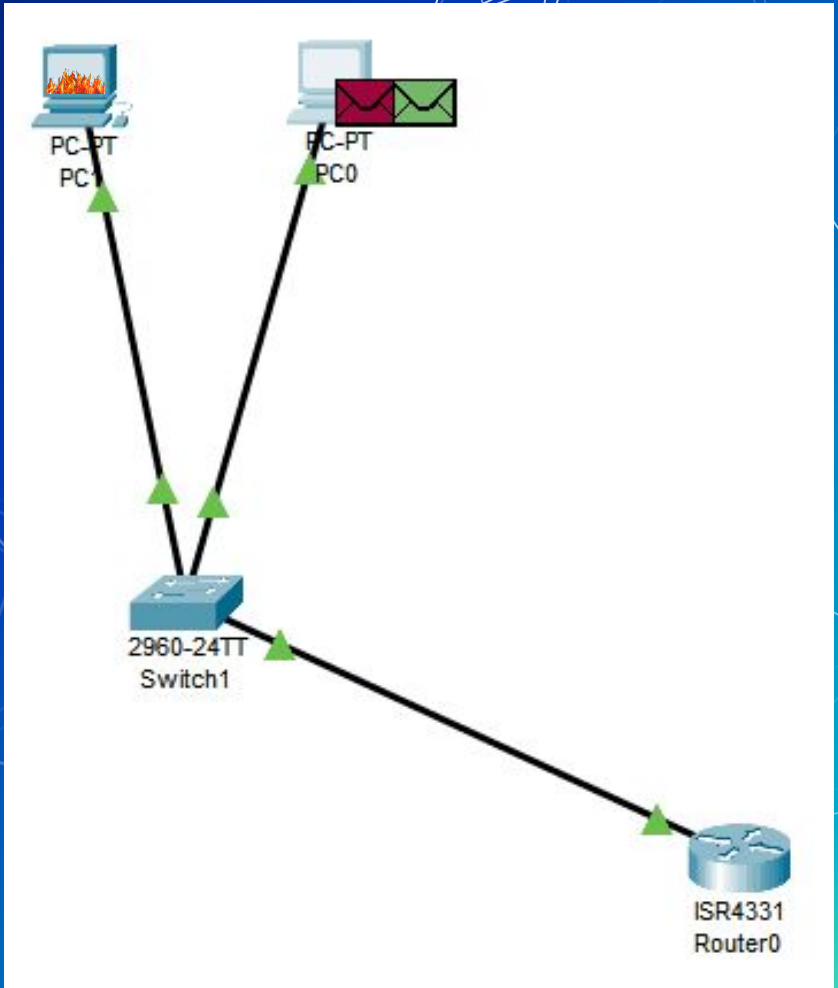
Activity – Host Based Firewalls

- Block all Ping requests using your Linux host based firewall.
  - Test by having someone at your table try to ping your device before and after
- Allow all ping requests using your Windows host based firewall.
  - Test by having someone at your table try to ping your device before and after.

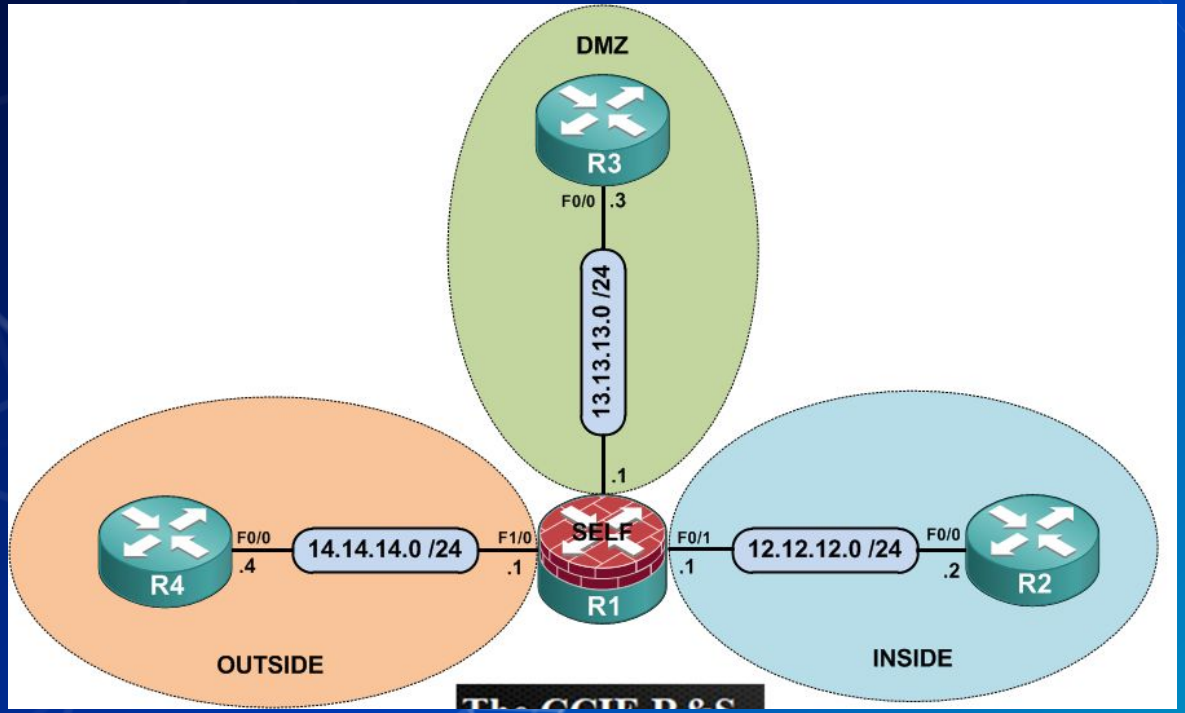
The Logic of Firewalls

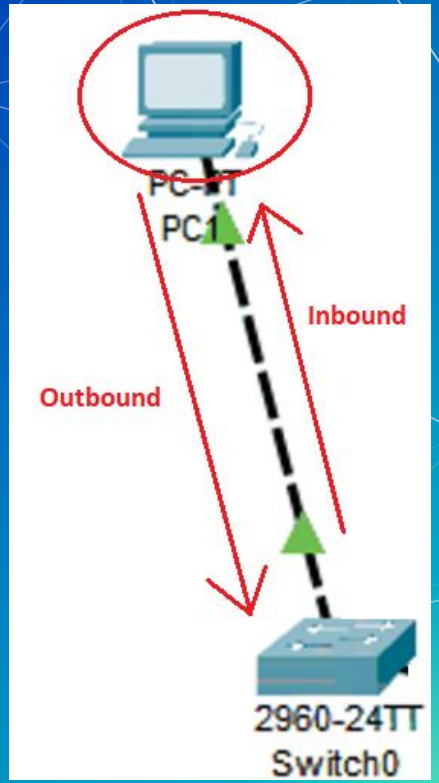
Data Flow

- Firewalls can regulate data flow



Zones


DMZ
R3
F0/0
.3
13.13.13.0 /24
.1
R4
F0/0
.4
14.14.14.0 /24
F1/0
.1
SELF
R1
F0/1
.1
12.12.12.0 /24
F0/0
.2
R2
OUTSIDE
INSIDE


PC1
Inbound
Outbound
2960-24TT
Switch0

Rule Hierarchy

- Each packet is checked against rules.
  - Packets are sent down the list. (Order Matters)
    - Packets can be:
      - Rejected
      - Dropped
      - Allowed

Floating WAN LAN

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✔	1 /2.30 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
☐	✖	0 /0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		HHTPS Traffic Block	
☐	✔	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	

Catch all rule

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

	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?

Compromised Device & PFSense Hands-On

Activity – PFSense Firewall

- Prevent all ping requests from inside your LAN to anywhere on the WAN (Anywhere on internet)
  - Test by attempting to ping 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 Domain Controller

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

Homework Prep

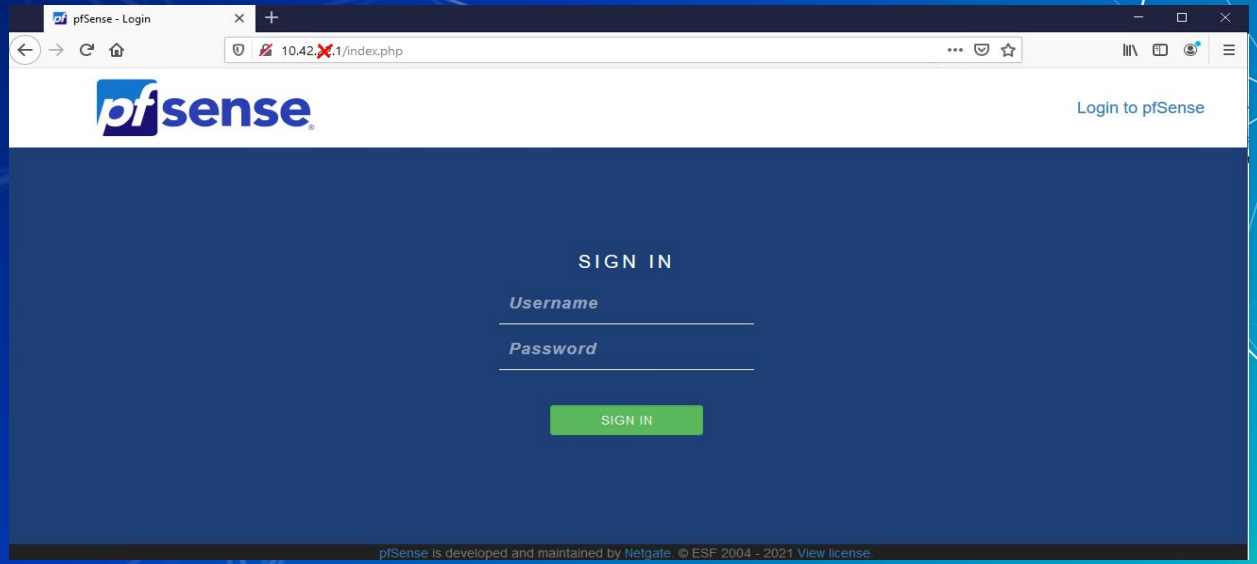
System Prep

- Prep 1: Install SSH on your Linux client
  - Package name: openssh-server
    - sudo apt install openssh-server
- Prep 2: Run script from GitHub on Windows Client (PrepareWindowsSystem.ps1)
  - https://github.com/ubnetdef/WindowsScriptsForLecture

Homework Starter

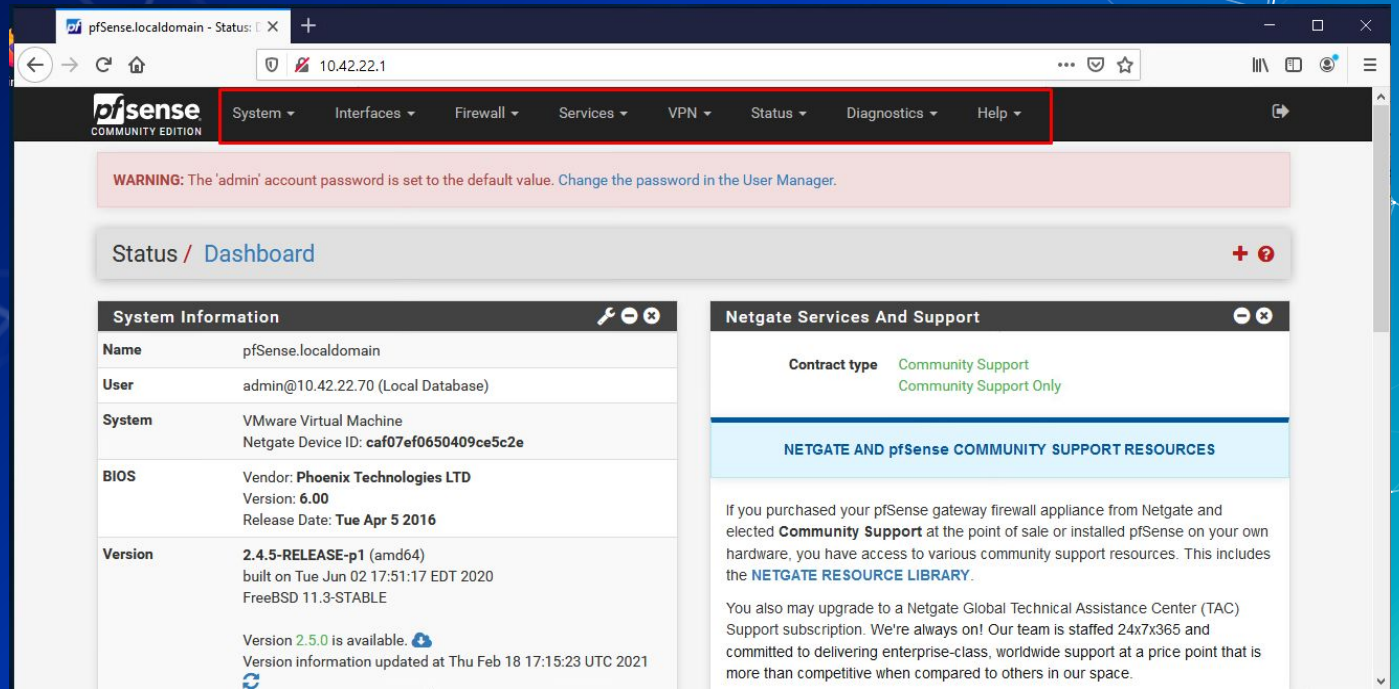
Homework Starter

- Credentials
  - Username: admin
  - Password: pfsense



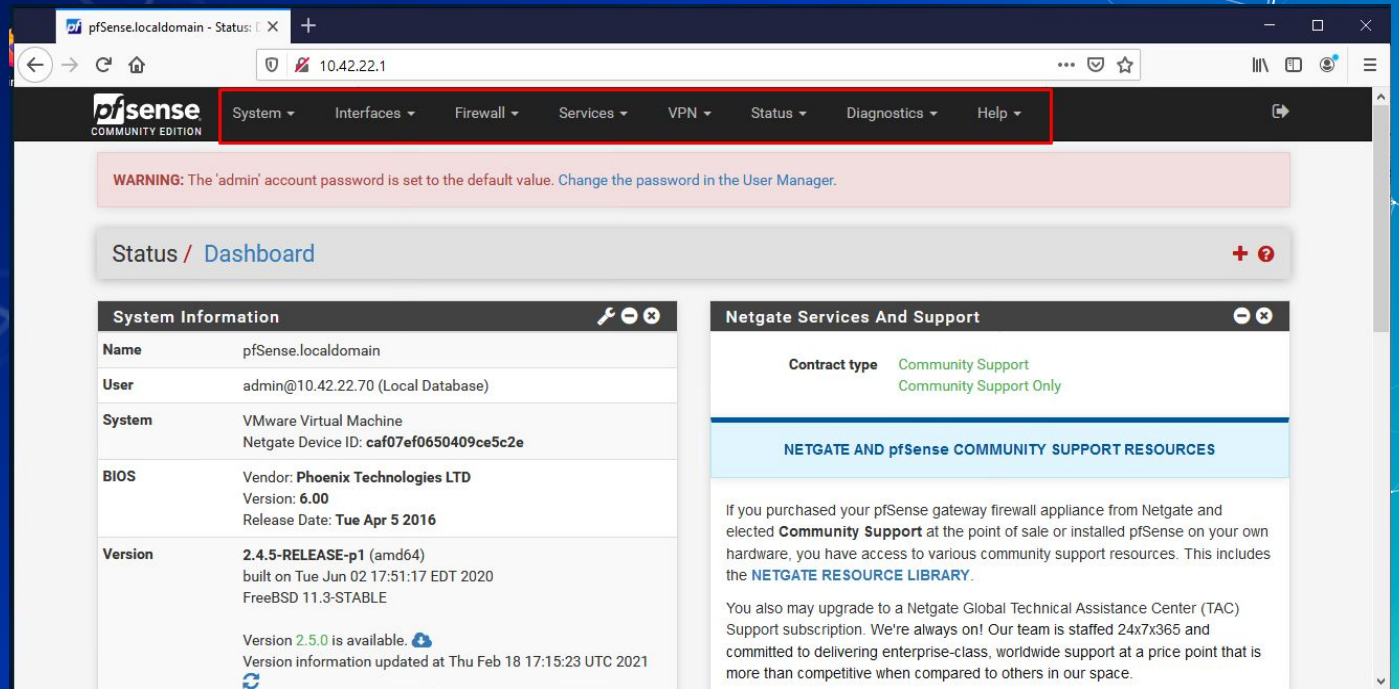
Homework Starter

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



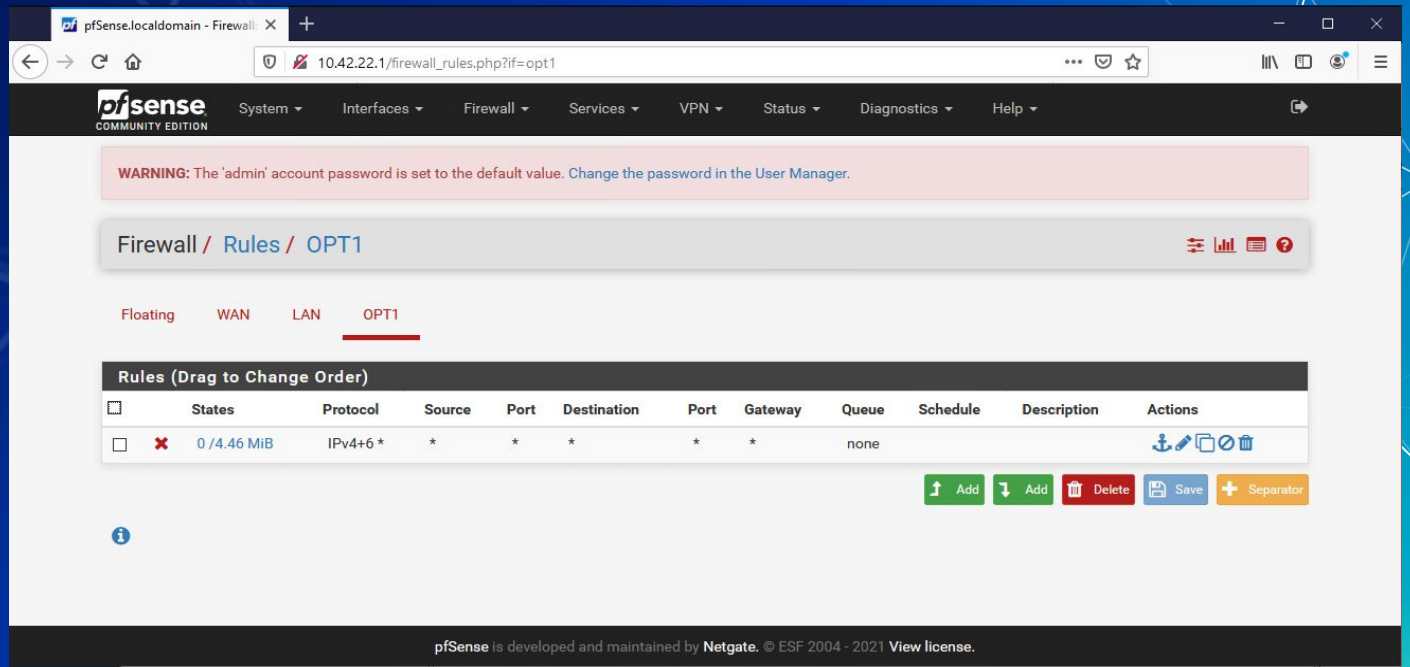
Homework Starter

- 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.