Firewalls

UBNetDef, Spring 2021

Week 3

Lead Presenter: Anthony Magrene

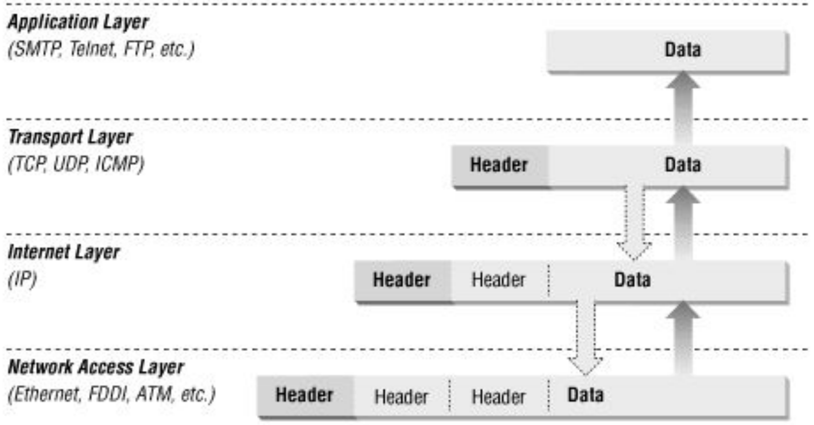
Agenda - Week 3

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

Networking Recap

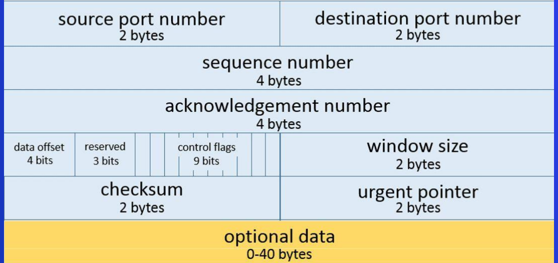
Networking Recap

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

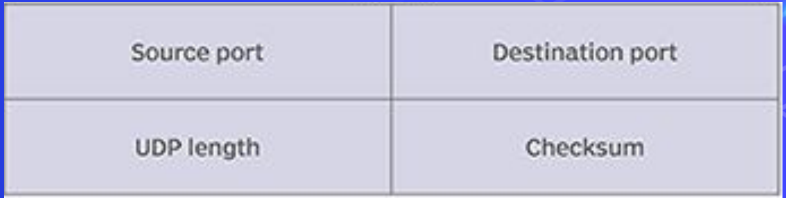


Networking Recap

- TCP has sessions
- UDP does not have sessions



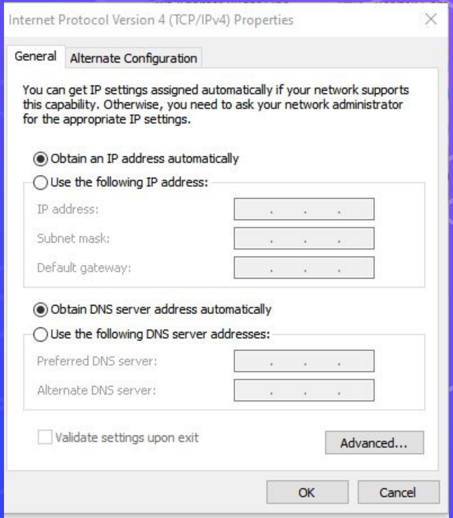
<table>
<tr><td colspan="3">source port number
2 bytes</td><td>destination port number
2 bytes</td></tr>
<tr><td colspan="4">sequence number
4 bytes</td></tr>
<tr><td colspan="4">acknowledgement number
4 bytes</td></tr>
<tr><td>data offset
4 bits</td><td>reserved
3 bits</td><td>control flags
9 bits</td><td>window size
2 bytes</td></tr>
<tr><td colspan="3">checksum
2 bytes</td><td>urgent pointer
2 bytes</td></tr>
<tr><td colspan="4">optional data
0-40 bytes</td></tr>
</table>



Source port	Destination port
UDP length	Checksum

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)



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

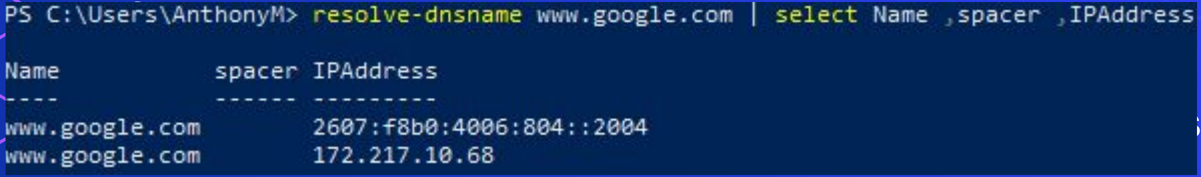
● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

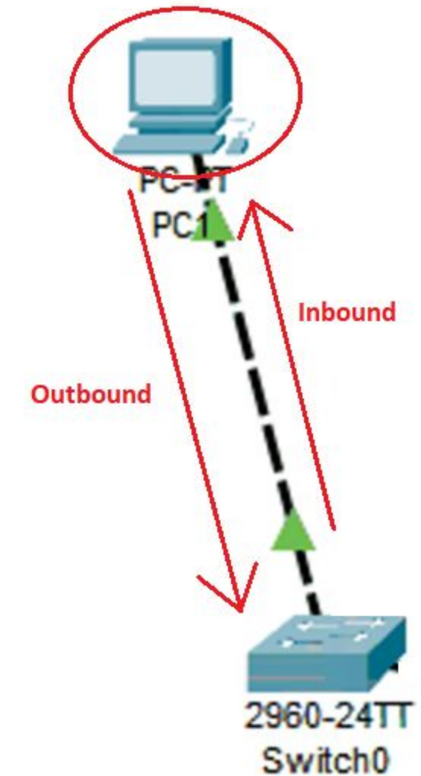


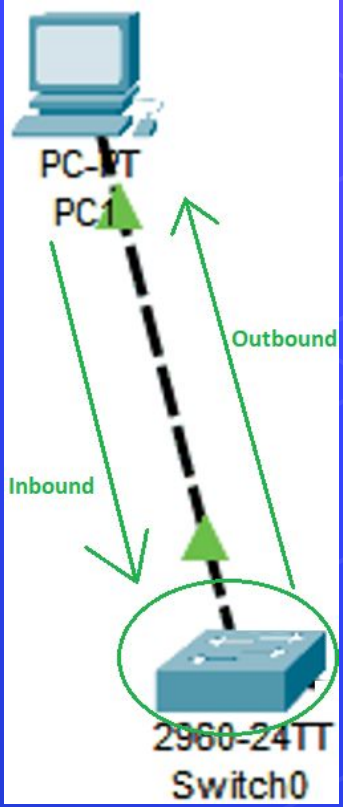
```
PS C:\Users\AnthonyM> resolve-dnsname www.google.com | select Name ,spacer ,IPAddress

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

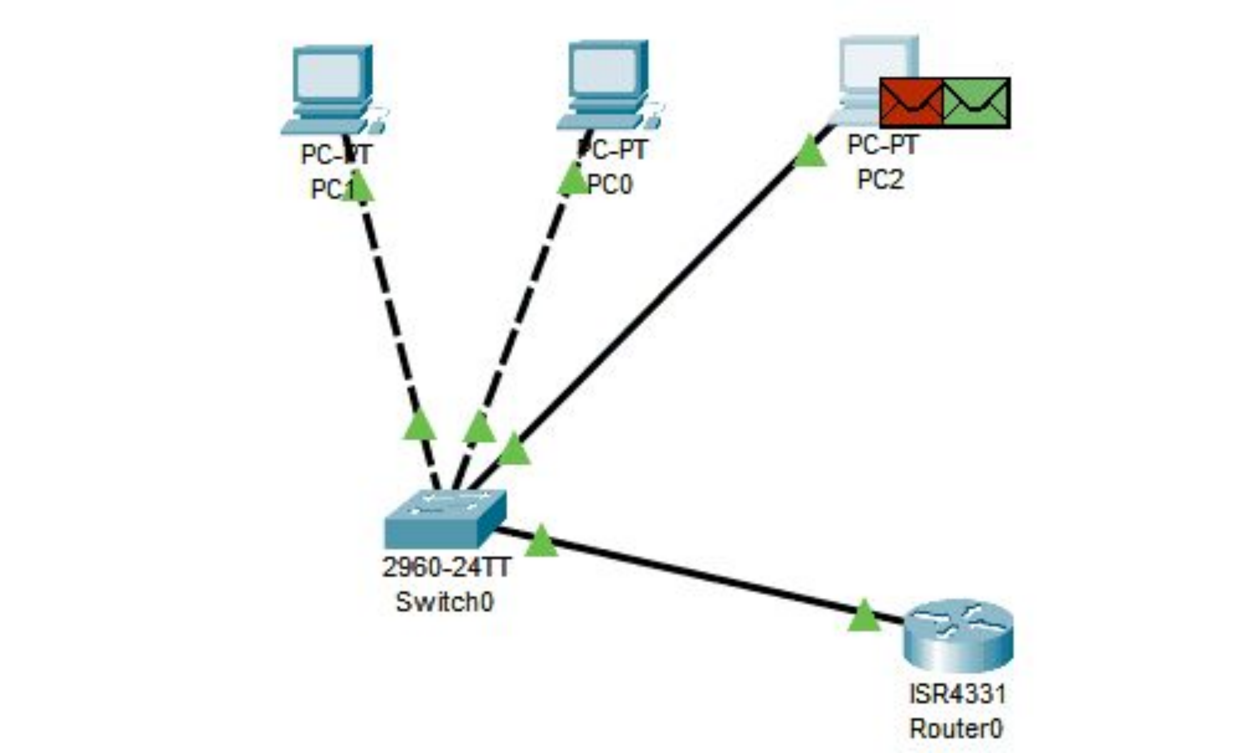
not required

Directional Flow





Data flows freely… for now



Networking Recap Questions?

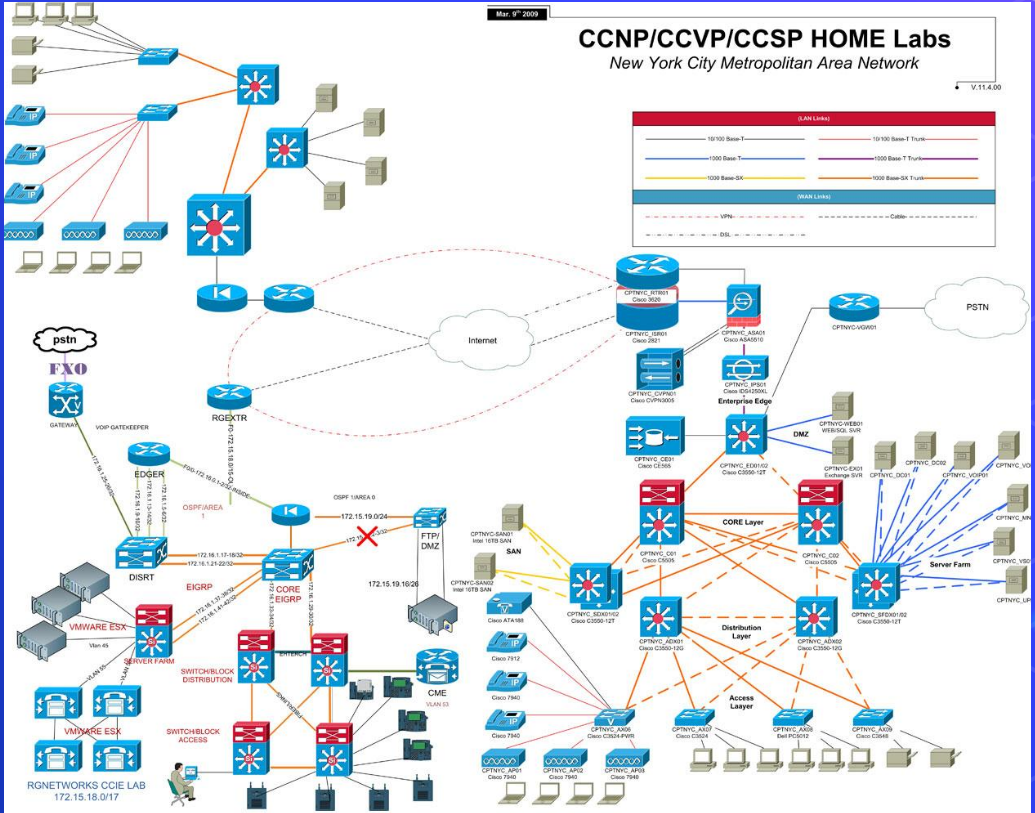
Hands on Migration

Activity – Migrate Linux to LAN

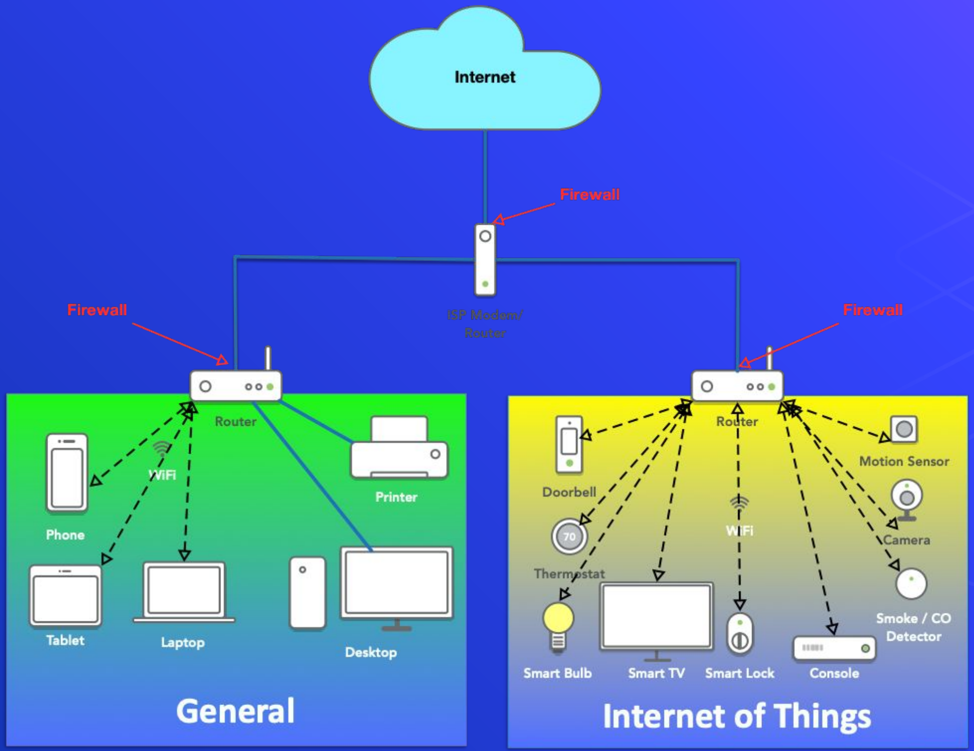
- Migrate your Linux client from your **DMZ** to the **LAN** network

Why Firewalls?

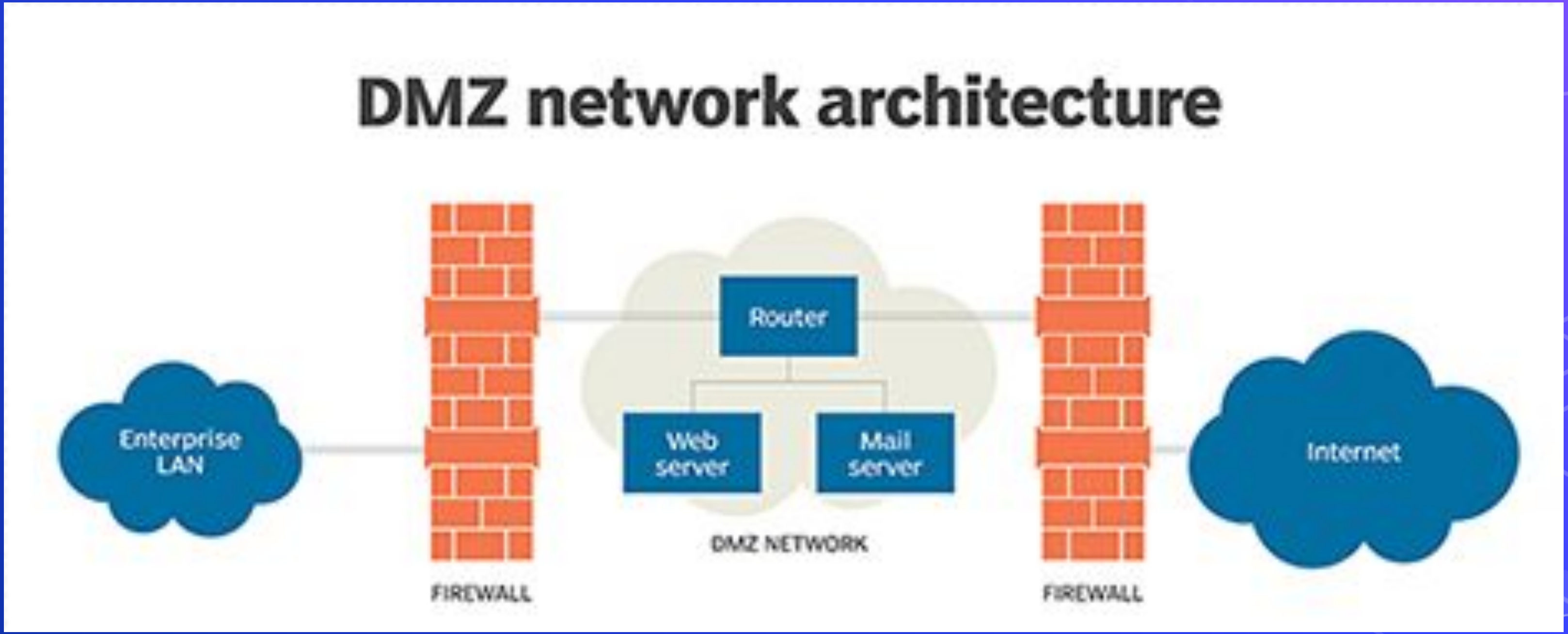
Why Firewalls?



Why Firewalls?



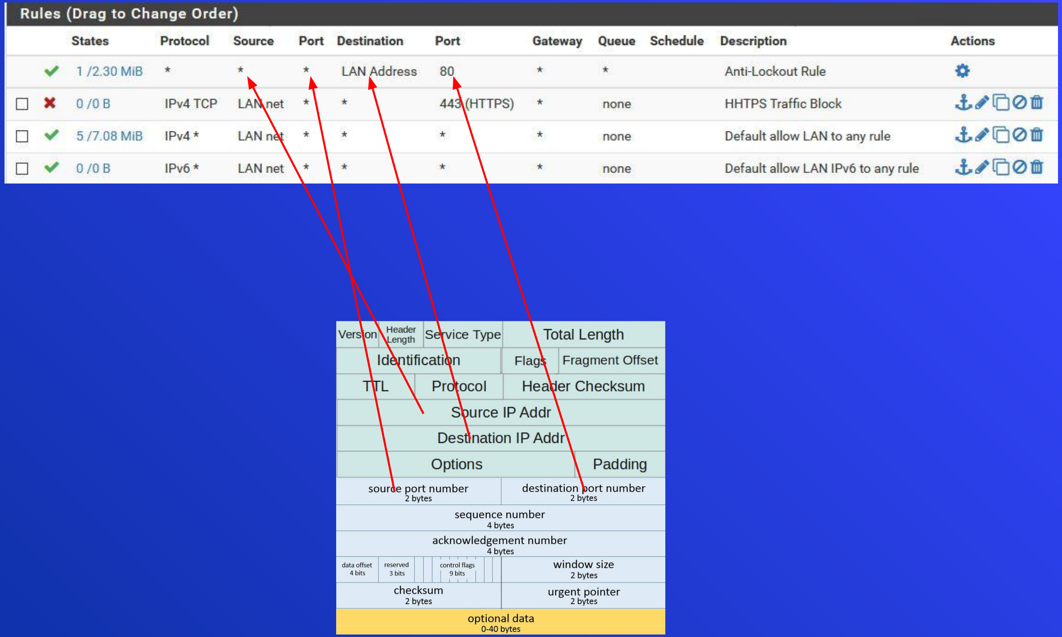
Why Firewalls?



Types of Firewalls

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

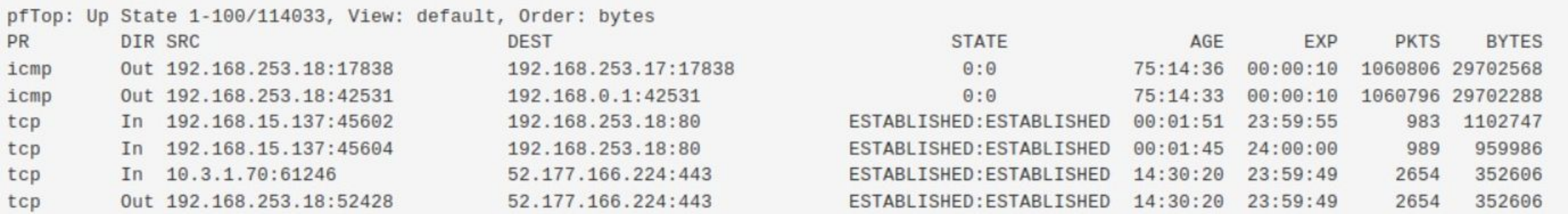
Packet Filters



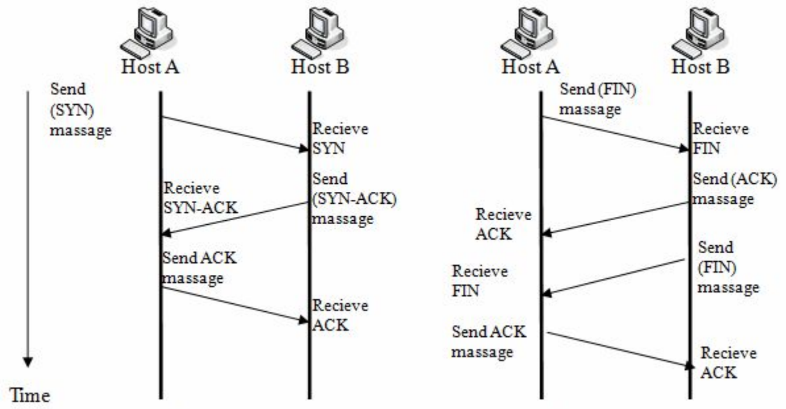
Rules (Drag to Change Order)

		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

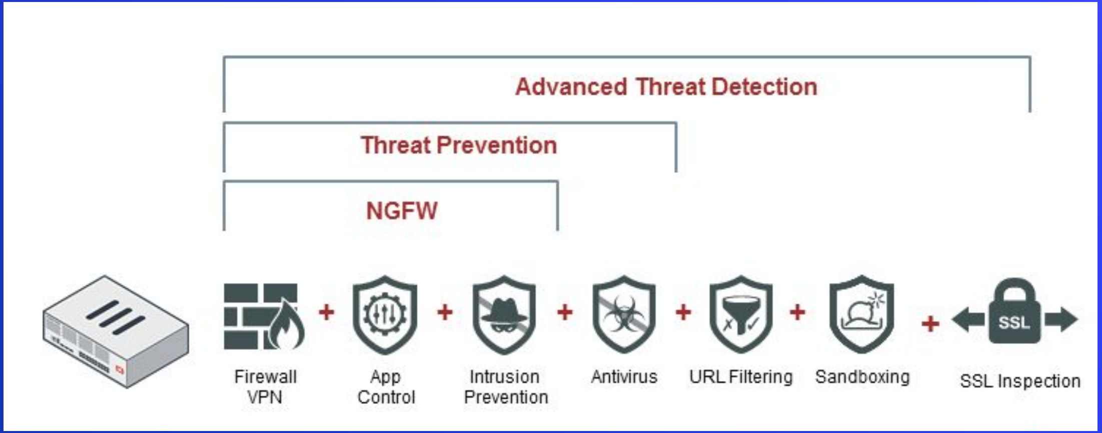


```
pfTop: Up State 1-100/114033, View: default, Order: bytes
PR         DIR SRC                             DEST                                        STATE                  AGE        EXP       PKTS     BYTES
icmp       Out 192.168.253.18:17838            192.168.253.17:17838                     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



NetDef

Next Generation Firewalls



pfsense

SOPHOS

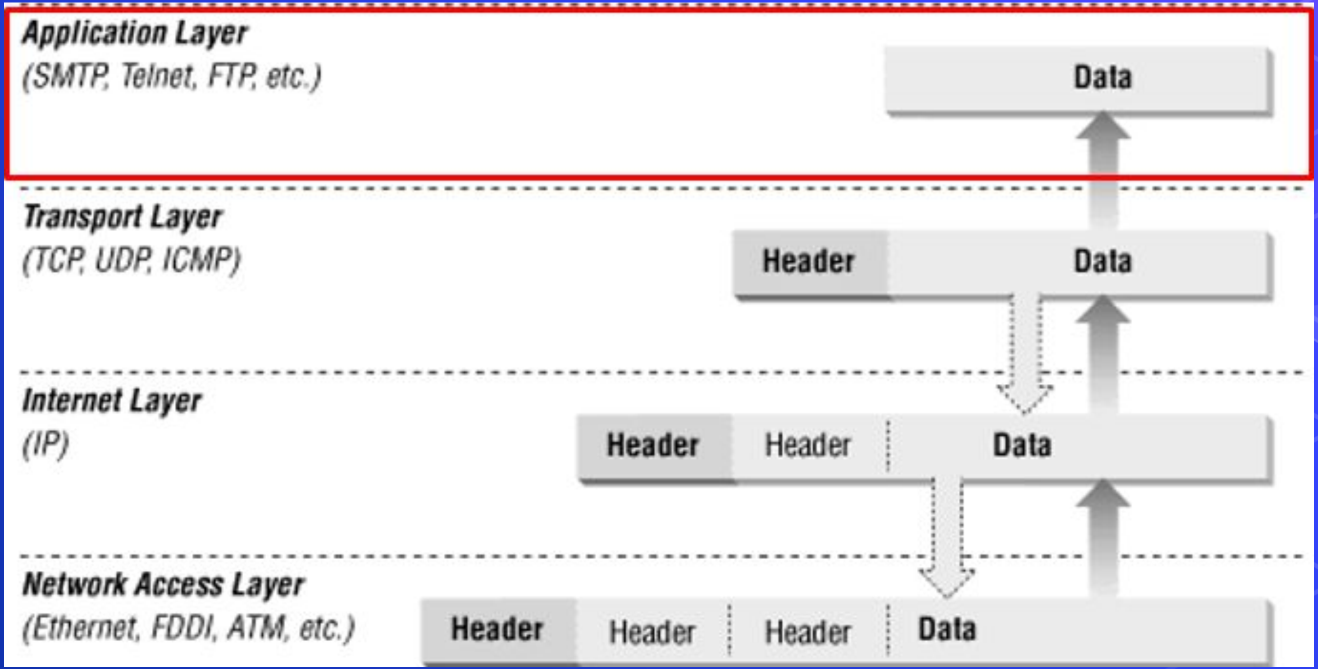
FORTINET

SONICWALL

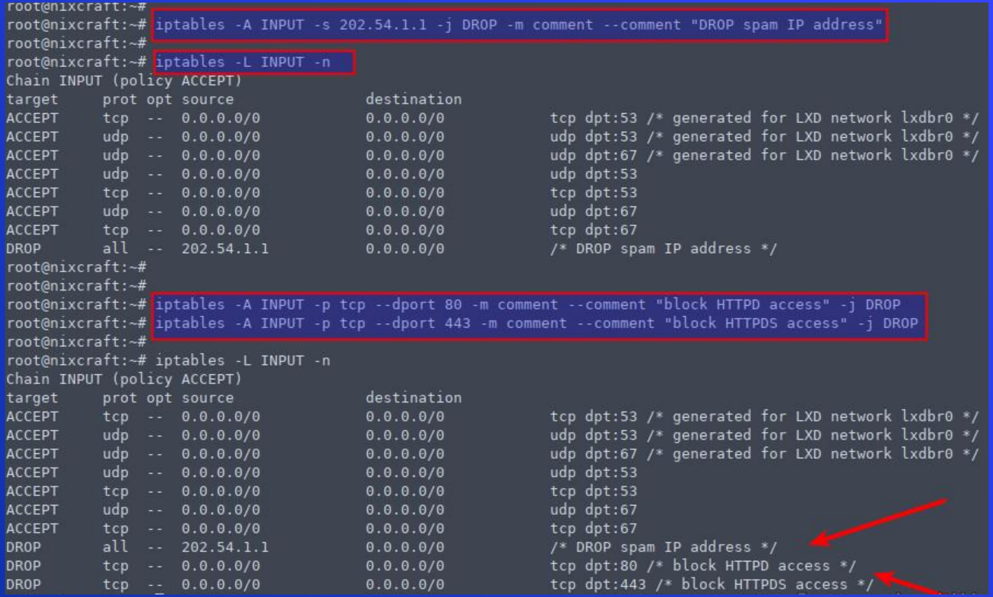
paloalto NETWORKS

Next Generation Firewalls cont.

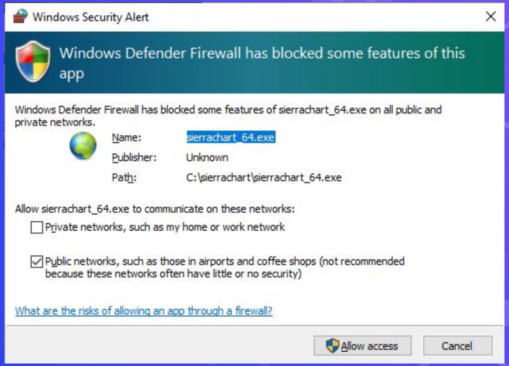
- Generally speaking most bad behavior happens in the application layer



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 */
```



Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of sierrachart_64.exe on all public and private networks.

Name: sierrachart_64.exe

Publisher: Unknown

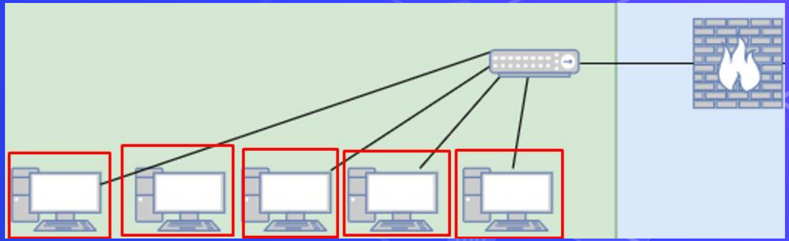
Path: C:\sierrachart\sierrachart_64.exe

Allow sierrachart_64.exe to communicate on these networks:

☐ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?



Host Based Firewalls Hands-On

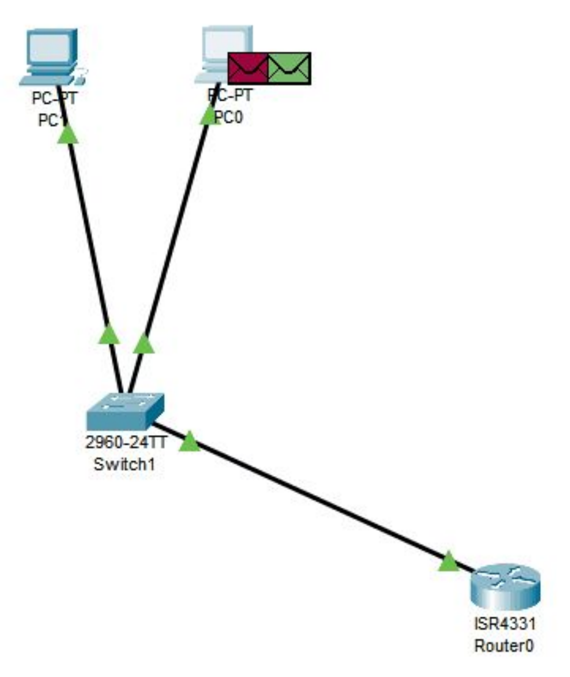
Activity – Host Based Firewalls

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

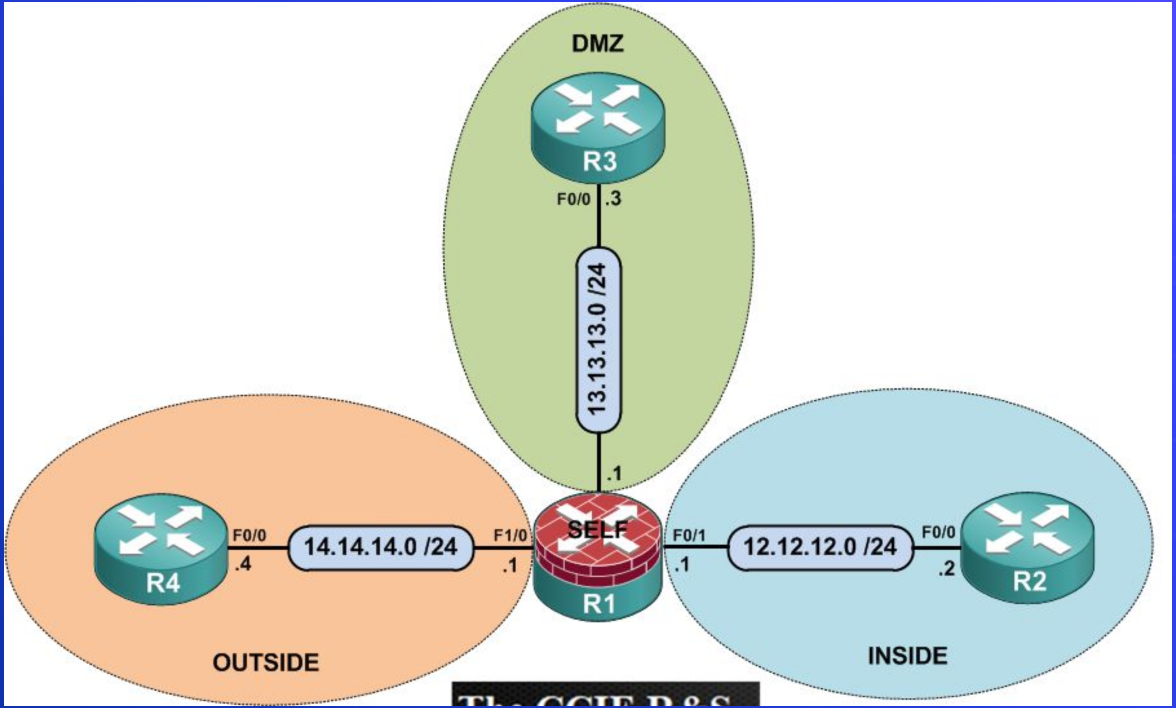
The Logic of Firewalls

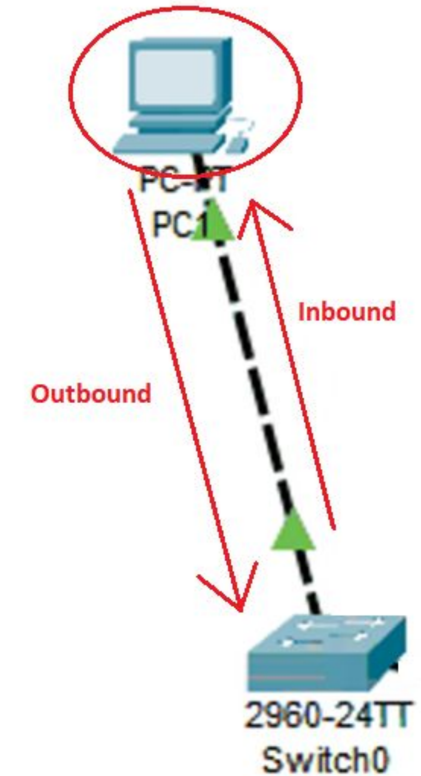
Data flow

- Data flows are regulated with firewalls



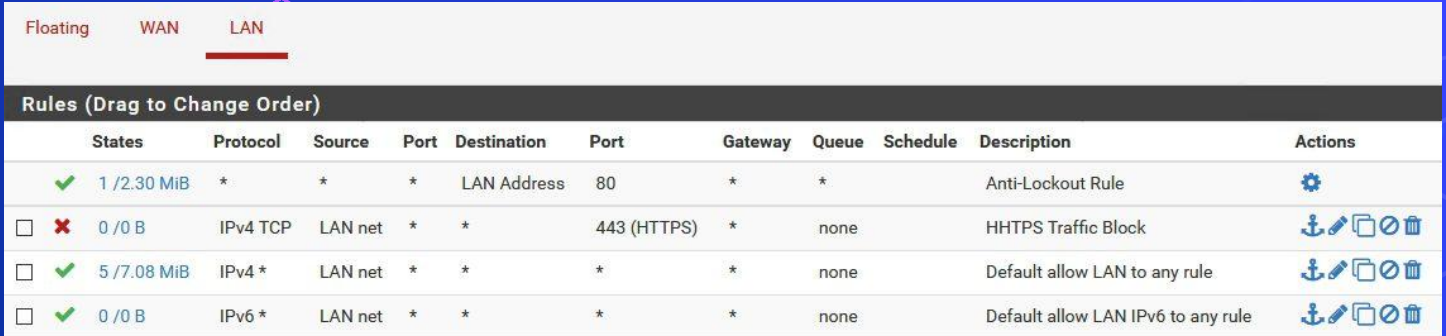
Zones


DMZ
R3
F0/0
.3
13.13.13.0 /24
.1
OUTSIDE
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
INSIDE
The CCIE R&S


PC-PT
PC1
Outbound
Inbound
2960-24TT
Switch0

Rule Hierarchy

- Each packet is checked against rules.
- In this case packets are sent down the list.
  - Packets can be:
    - Rejected



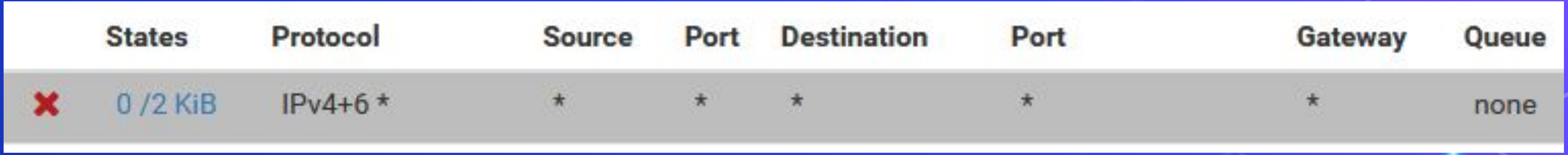
Floating WAN LAN

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	⚓ ✎ ⧉ ⊘ 🗑

Default Deny ALL

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

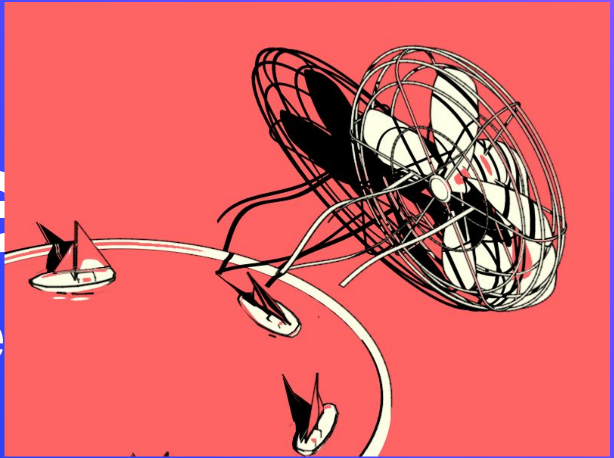


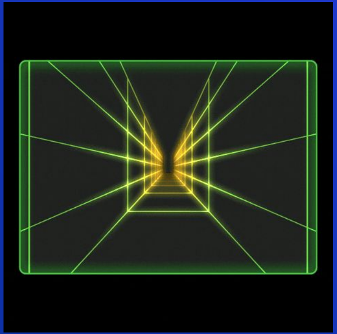
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
✖	0 /2 KiB	IPv4+6 *	*	*	*	*	*	none

Logic of Firewalls
Questions?

Break slide

Please return on time





Hands On

Activity – PFSense Firewall

- Prevent all ping requests from inside your LAN to anywhere on the WAN
  - 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 remote control protocols that Windows uses?

Homework Prep

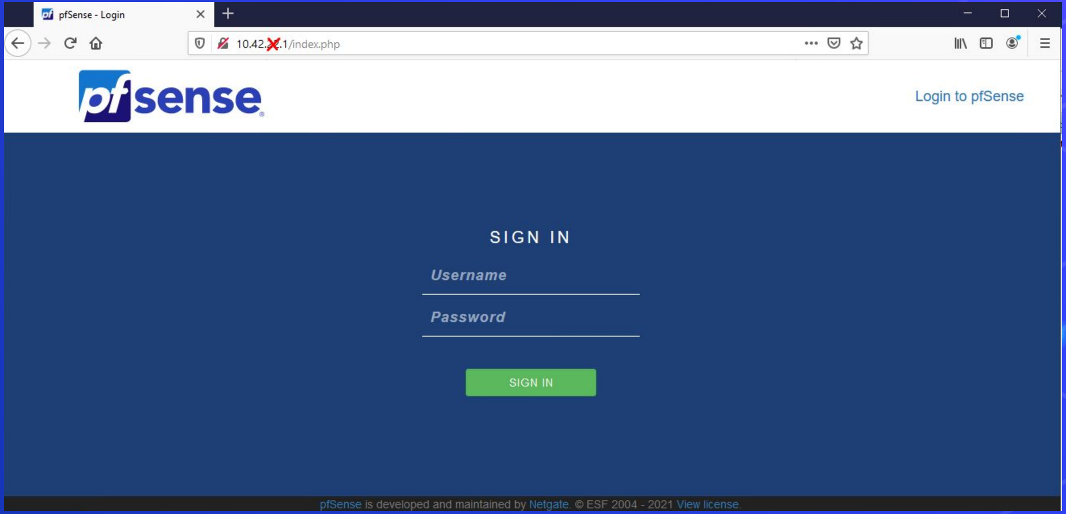
System Prep

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

Homework Starter

Homework Starter

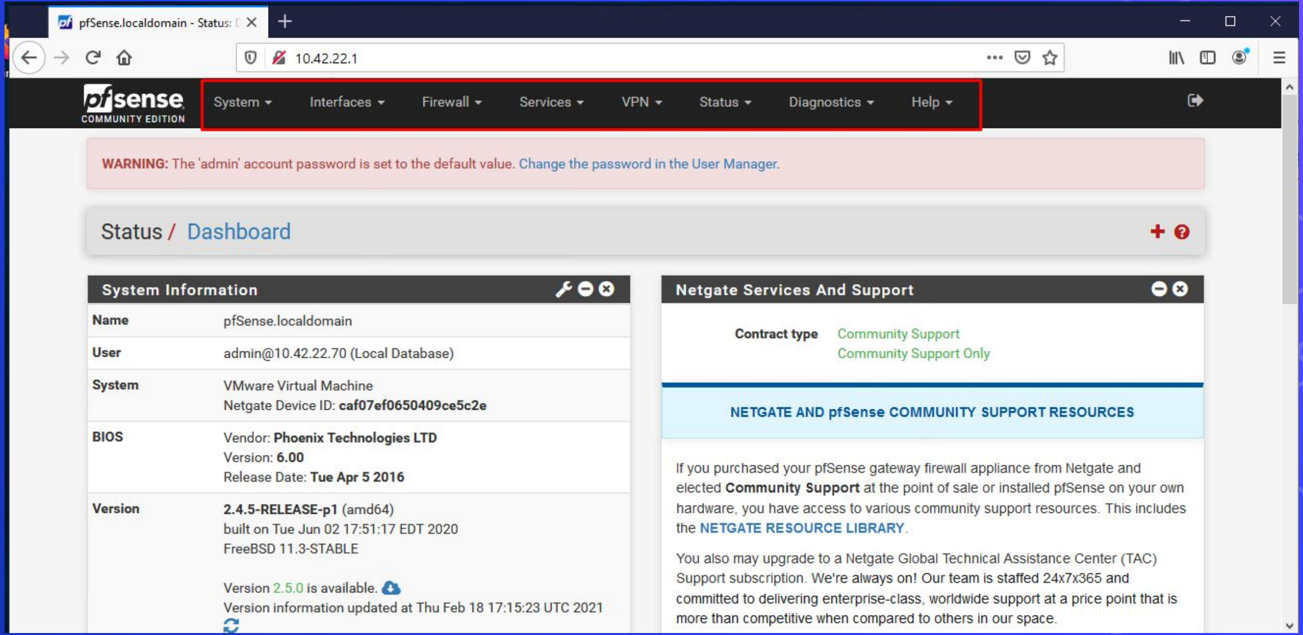
- Credentials
  - Username: admin
  - Password: pfsense



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

Homework Starter

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



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. Version information updated at Thu Feb 18 17:15:23 UTC 2021

Netgate Services And Support

Contract type	Community Support Community Support Only

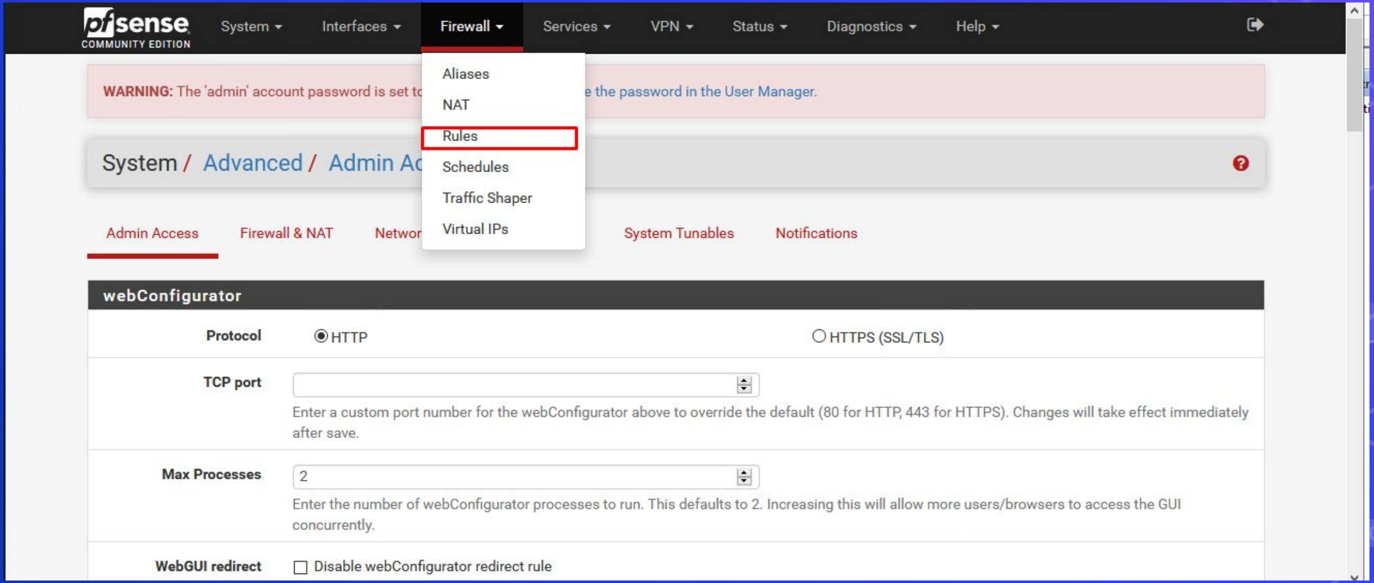
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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 menu is under Firewall > Rules



WARNING: The 'admin' account password is set to … e the password in the User Manager.

System / Advanced / Admin Ac

Admin Access | Firewall & NAT | Networ… | System Tunables | Notifications

webConfigurator

Protocol ● HTTP ○ HTTPS (SSL/TLS)

TCP port

Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

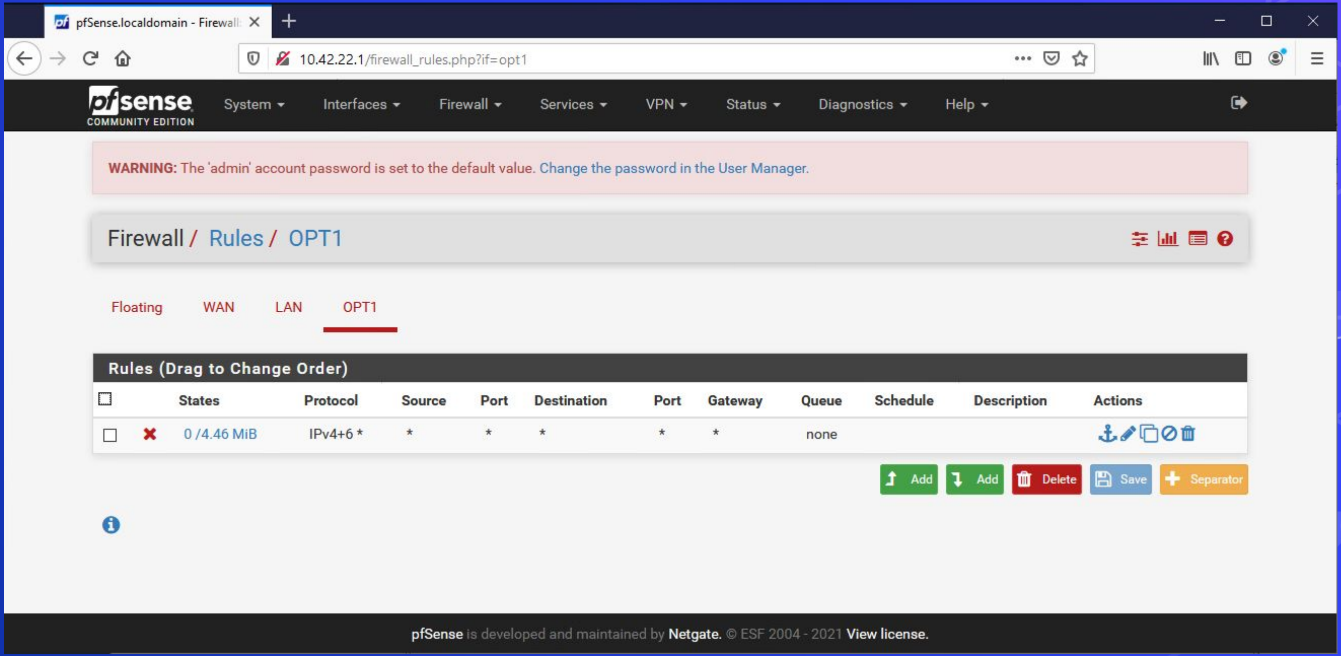
Max Processes 2

Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect □ Disable webConfigurator redirect rule

Homework Starter

- Rules are grouped by the interface that handles the packets



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / OPT1

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✖	0 /4.46 MiB	IPv4+6 *	*	*	*	*	*	none			

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

Homework Starter

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.