

Firewalls

UBNetDef, Fall 2021
Week 3

Lead Presenter:
Anthony Magrene

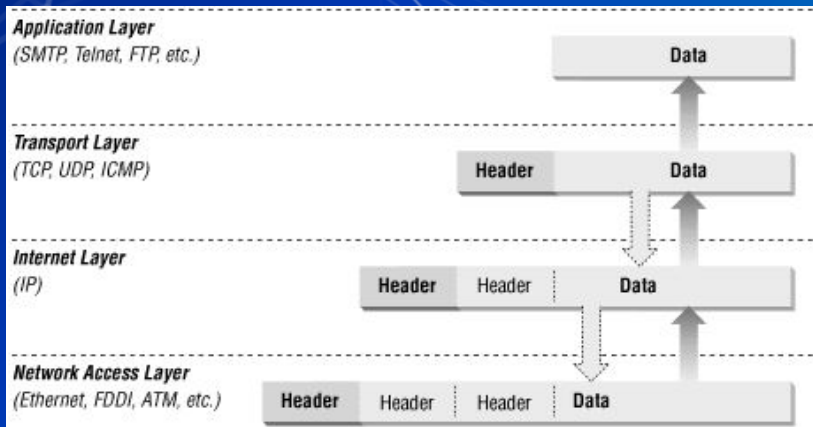
Agenda – Week 3

- 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

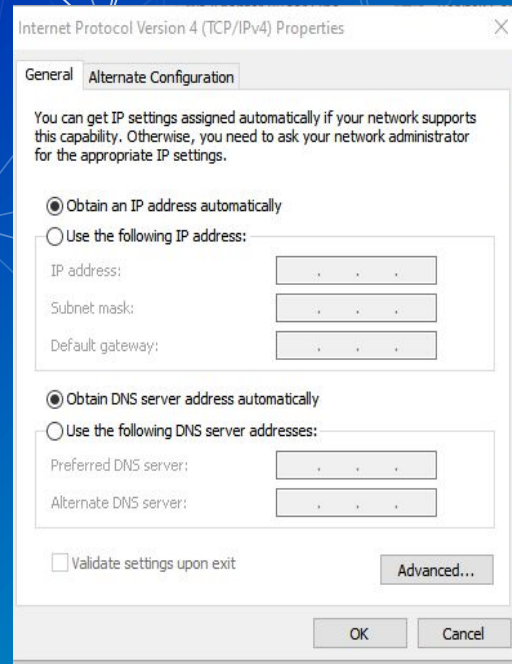
- TCP has sessions
- UDP does not have sessions

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							

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)
- Default gateway is where data must go to leave our LAN
- Domain Name Service makes life easy for us but is not required



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

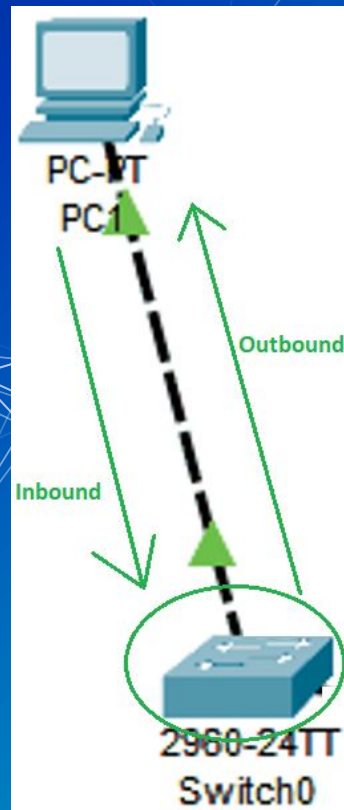
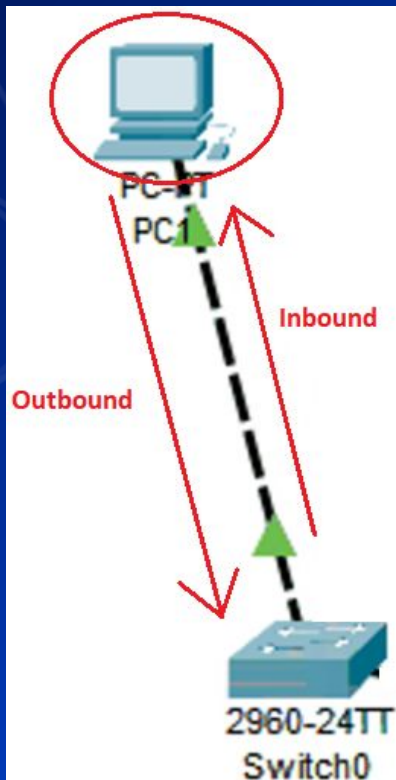
Advanced...

OK Cancel

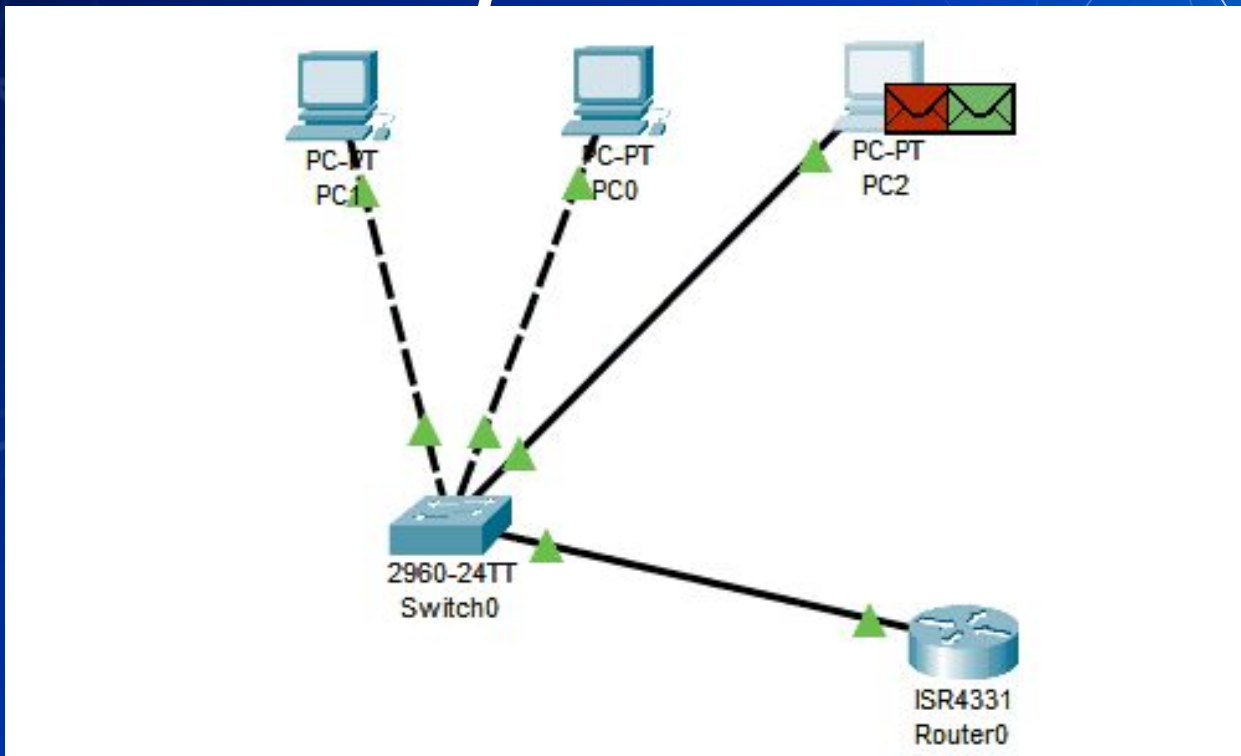
```
PS C:\Users\AnthonyM> resolve-dnsname www.google.com | select Name ,spacer ,IPAddress

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

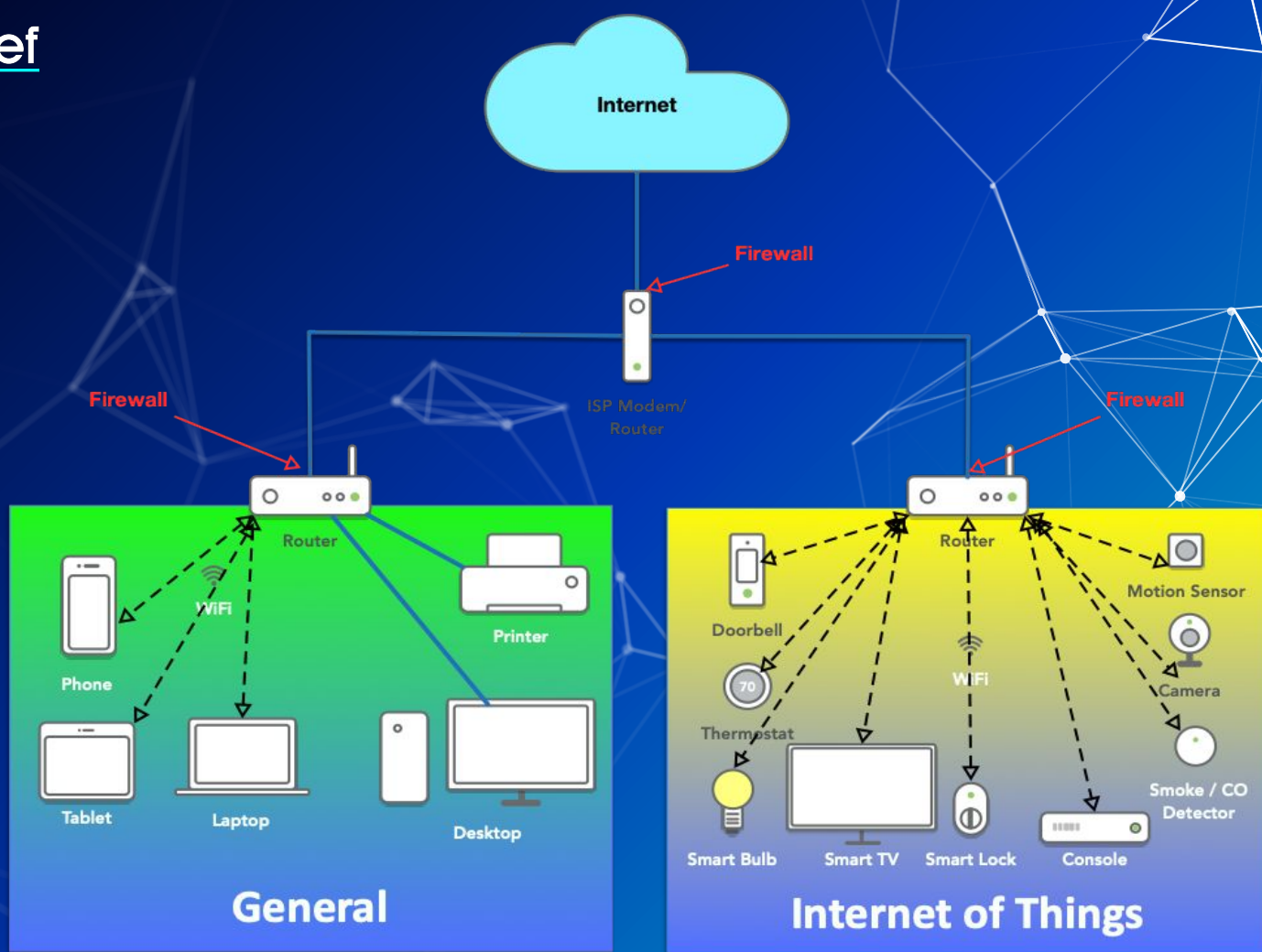
- Migrate your Windows client from your **DMZ** to the **LAN** network

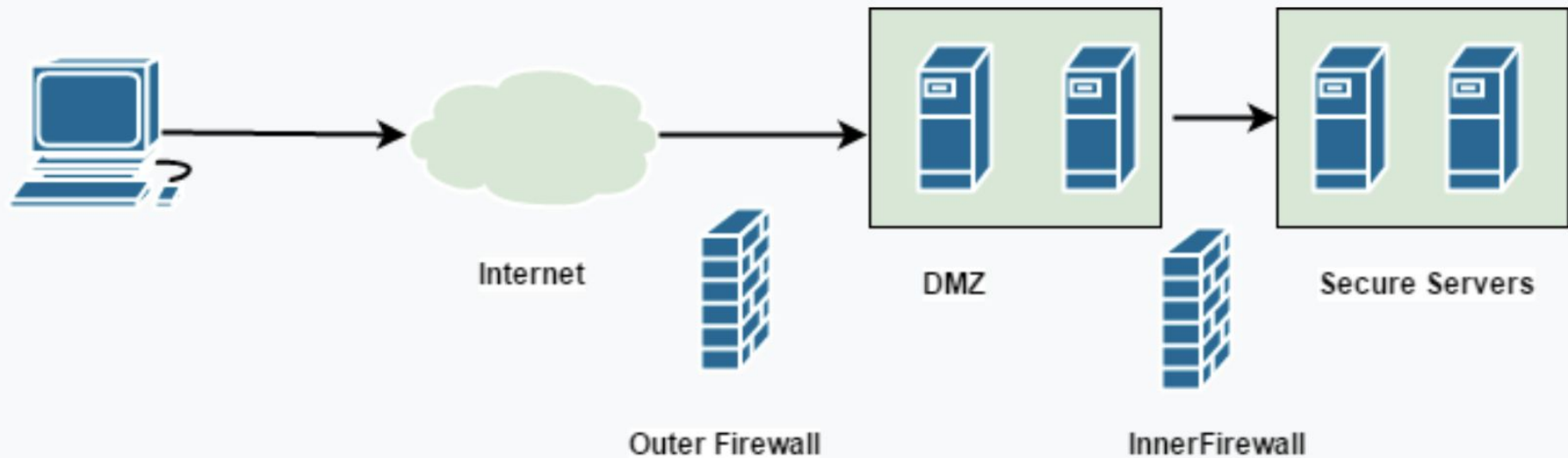
Why Firewalls?

New York City Metropolitan Area Network

V.11.4.00







DMZ

Types of Firewalls

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

Packet Filters

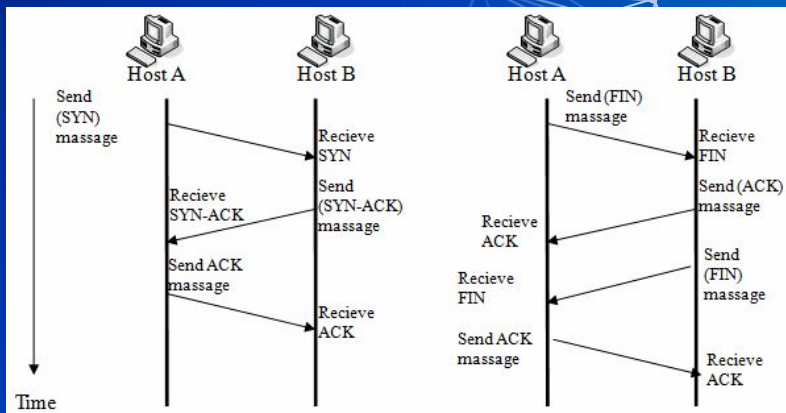
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 2.30 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		HTTPS Traffic Block	🔗✎📄🗑️
<input type="checkbox"/>	✓ 5 / 7.08 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗✎📄🗑️
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗✎📄🗑️

Version	Header Length	Service Type	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source IP Addr				
Destination IP Addr				
Options			Padding	
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				

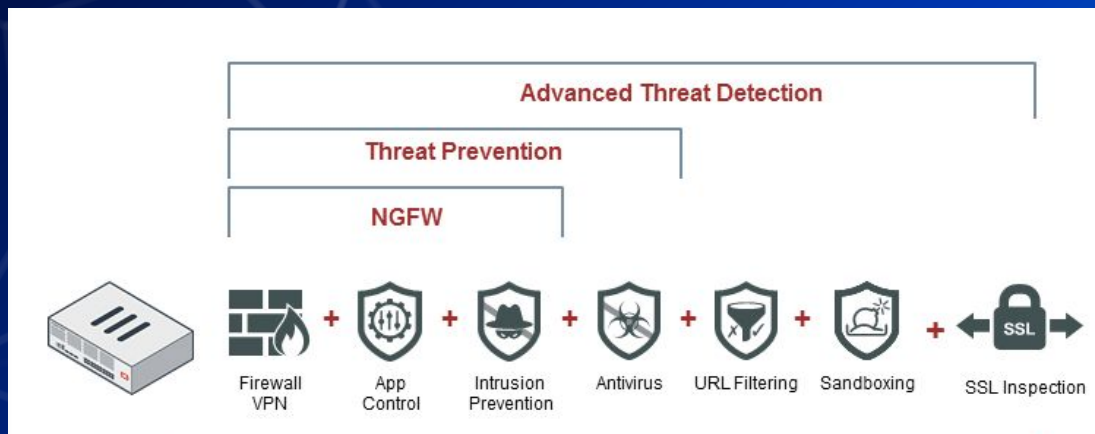
Stateful Firewalls

pfTop: Up State 1-100/114033, View: default, Order: bytes

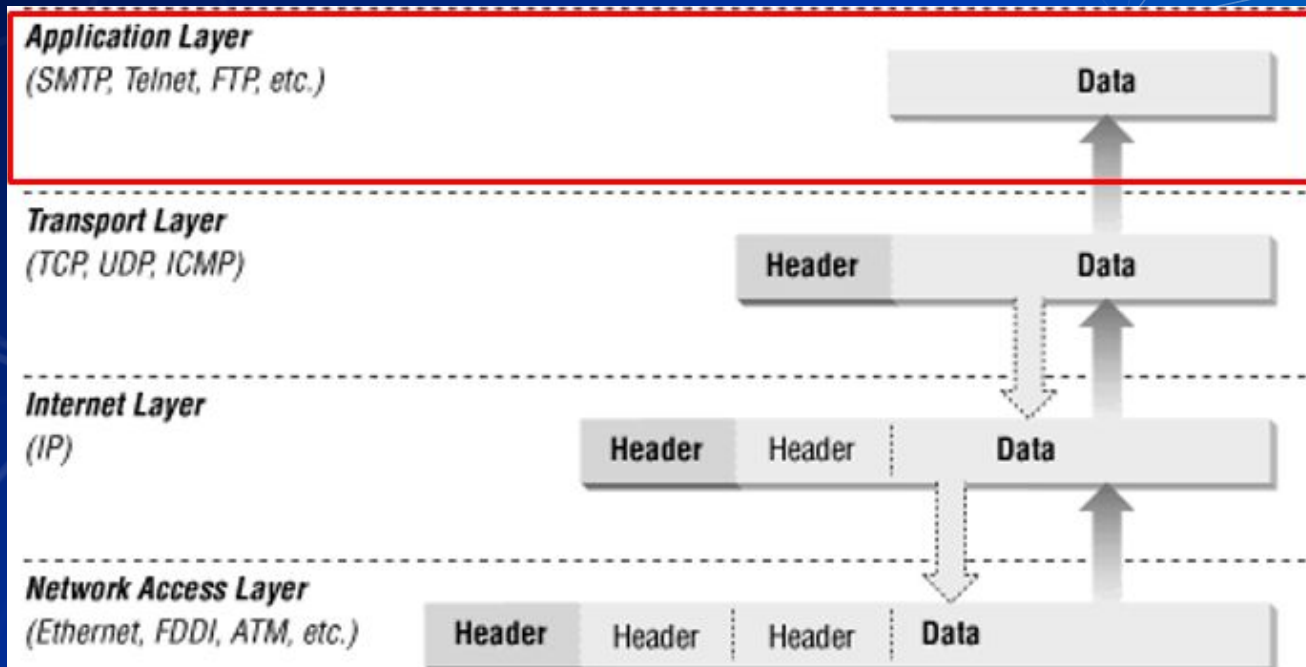
PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
icmp	Out	192.168.253.18:17838	192.168.253.17:17838	0:0	75:14:36	00:00:10	1060806	29702568
icmp	Out	192.168.253.18:42531	192.168.0.1:42531	0:0	75:14:33	00:00:10	1060796	29702288
tcp	In	192.168.15.137:45602	192.168.253.18:80	ESTABLISHED:ESTABLISHED	00:01:51	23:59:55	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



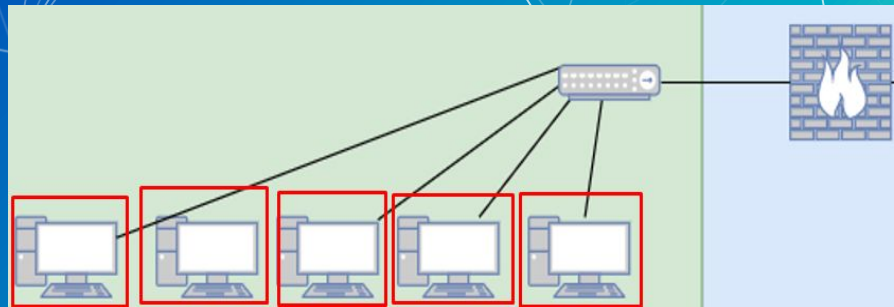
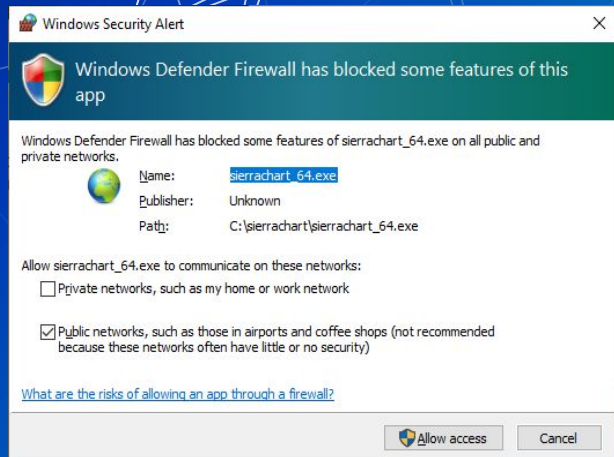
Next Generation Firewalls cont.



Host based Firewalls

```
root@nixcraft:~# 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 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: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
DROP all -- 202.54.1.1 0.0.0.0/0 /* DROP spam IP address */

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 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: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
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 */
```



Host Based Firewalls Hands-On

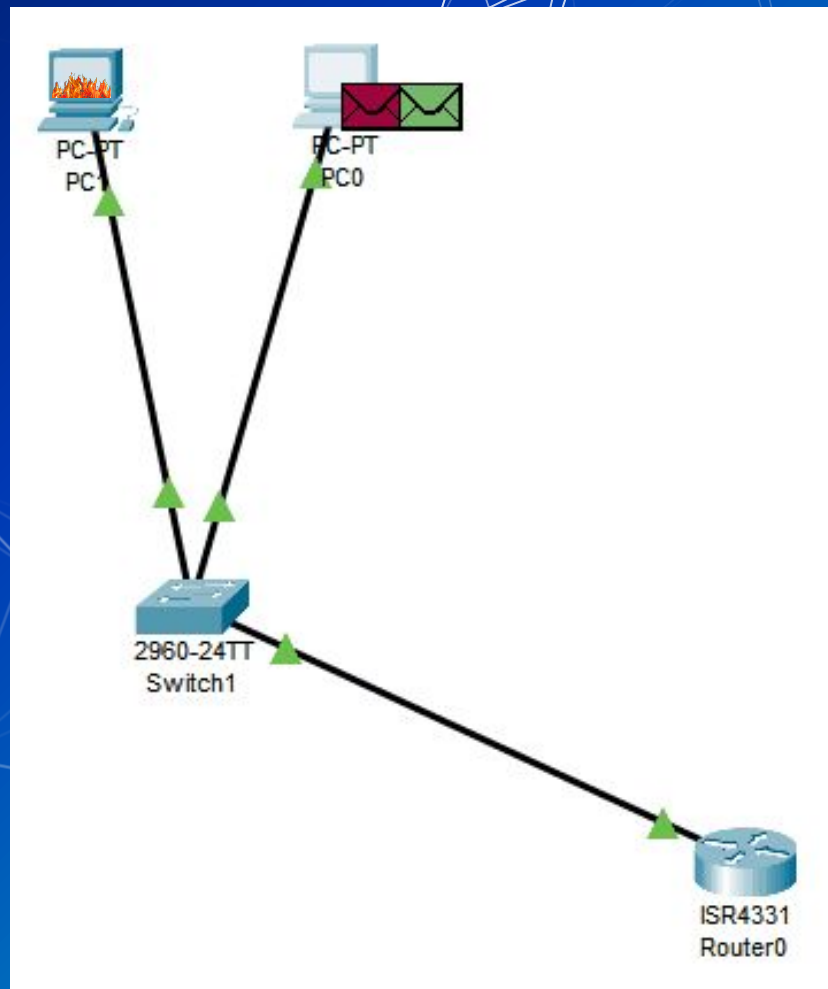
Activity – Host Based Firewalls

- 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.

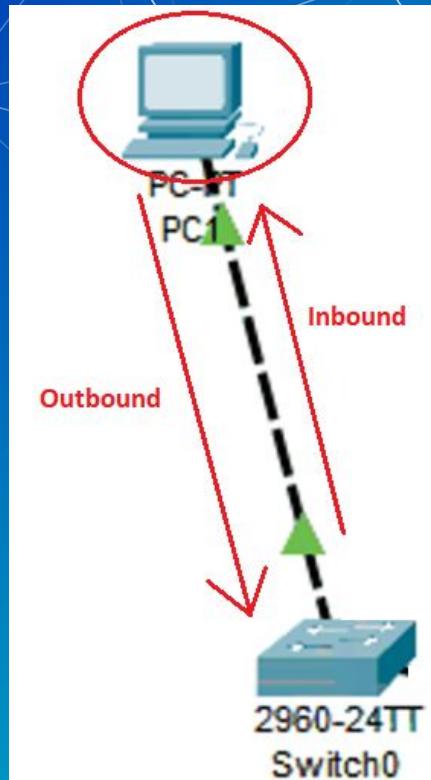
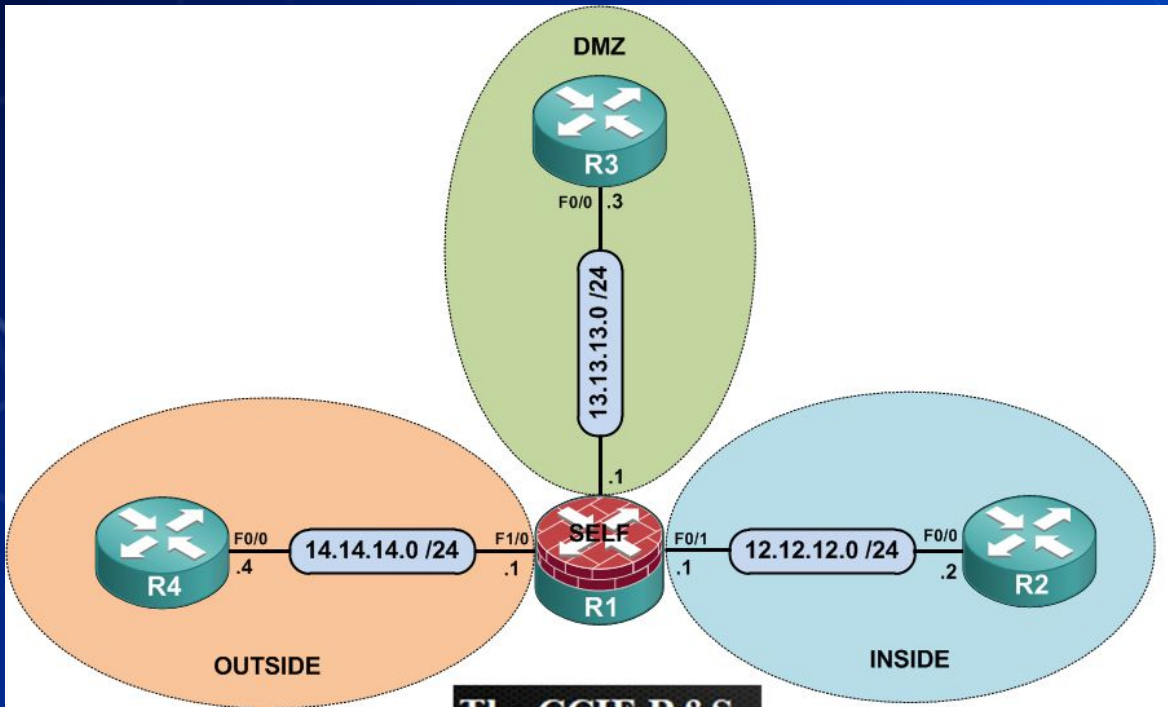
The Logic of Firewalls

Data Flow

- Firewalls can regulate data flow



Zones



Rule Hierarchy

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

Floating WAN <u>LAN</u>											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1 / 2.30 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none		HHTTPS Traffic Block	
<input type="checkbox"/>	✓ 5 / 7.08 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 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

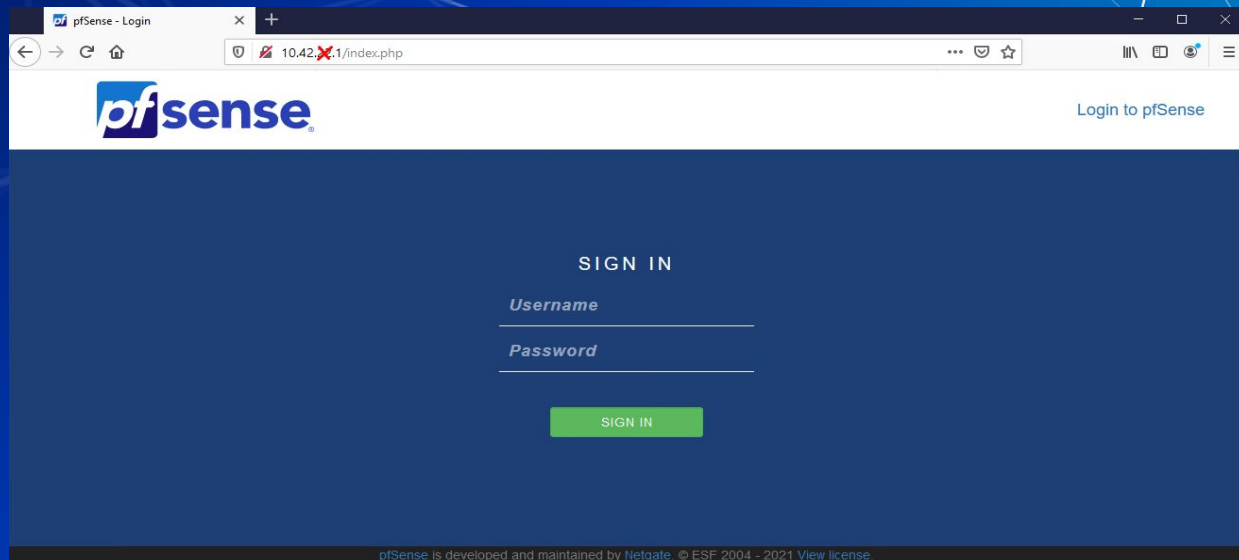
- Prep 1: Install SSH on your Linux client
 - Package name: openssh-server
 - `sudo apt install openssh-server`
- Prep 2: Run script from GitHub on Windows Client (PrepareWindowsSystem.ps1)
 - <https://github.com/ubnetdef/WindowsScriptsForLecture>

Homework Starter

Homework Starter

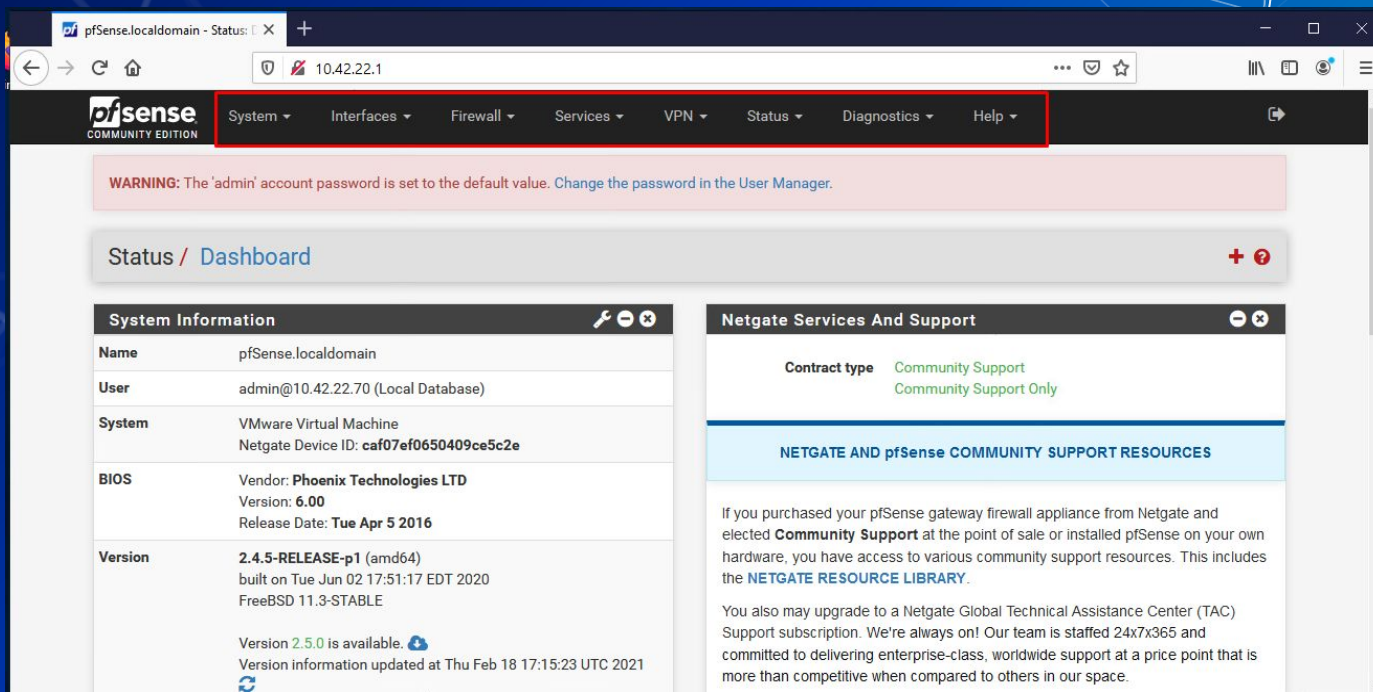
■ Credentials

- Username: admin
- Password: pfsense



Homework Starter

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



pfSense.localdomain - Status | 10.42.22.1

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

Netgate Services And Support

Contract type **Community Support**
Community Support Only

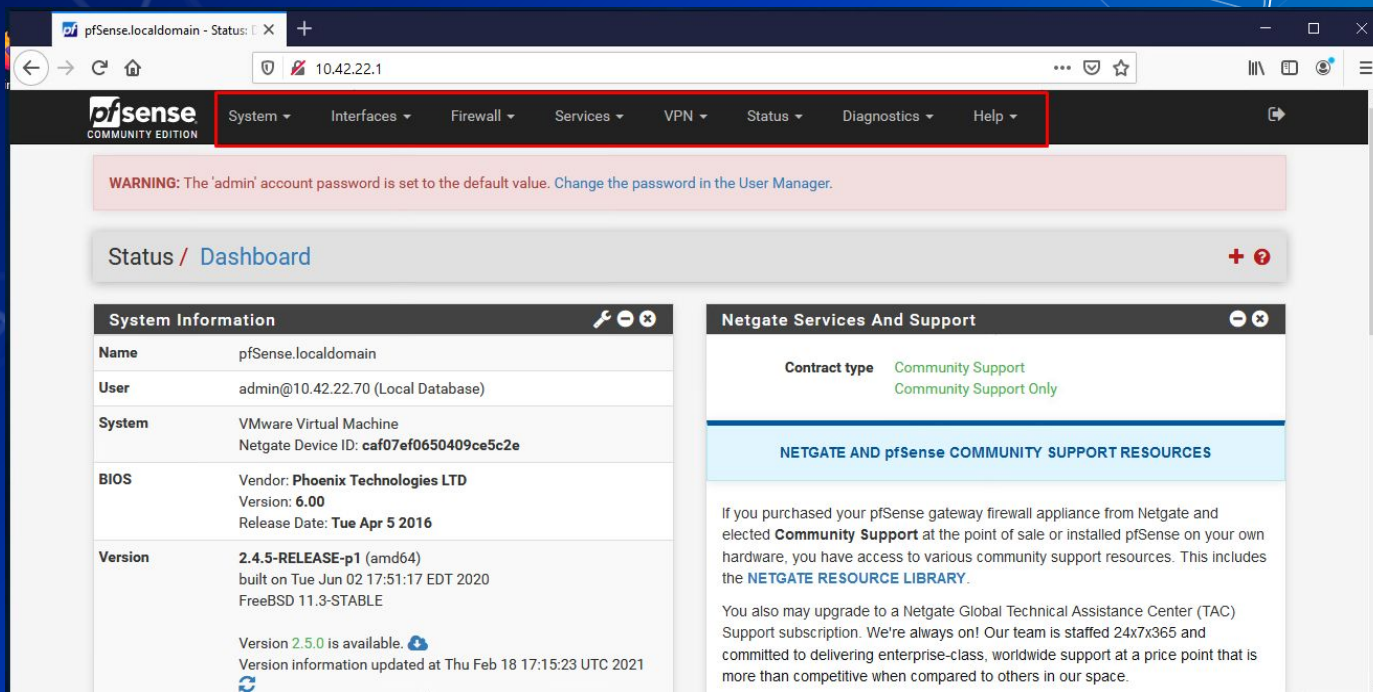
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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



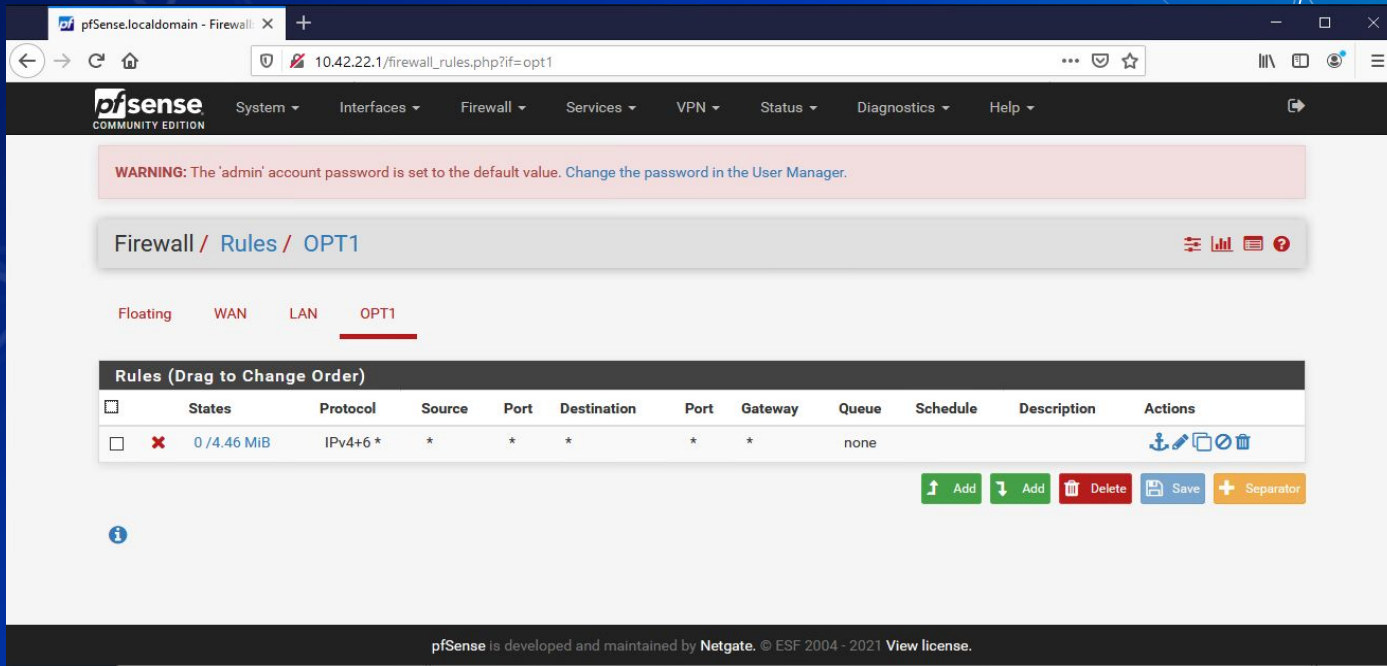
The screenshot shows the pfSense web interface in a browser window. The browser's address bar displays '10.42.22.1'. The pfSense header bar includes a navigation menu with the following items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red rectangular box highlights the 'Firewall' and 'Help' items in this menu. Below the header, 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'. It is divided into two columns. The left column, 'System Information', contains a table with the following data:

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

The right column, 'Netgate Services And Support', displays the 'Contract type' as 'Community Support' and 'Community Support Only'. Below this, a section titled 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' provides information about community support resources and the option to upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription.

Homework Starter

- Rules are grouped by the interface that handles the packets



The screenshot shows the pfSense Community Edition web interface. The browser address bar displays `10.42.22.1/firewall_rules.php?if=opt1`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail is Firewall / Rules / OPT1. Below this, tabs for Floating, WAN, LAN, and OPT1 are shown, with OPT1 selected. The main section is titled "Rules (Drag to Change Order)". It contains a table with the following data:

	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 are buttons: Add (up arrow), Add (down arrow), 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.