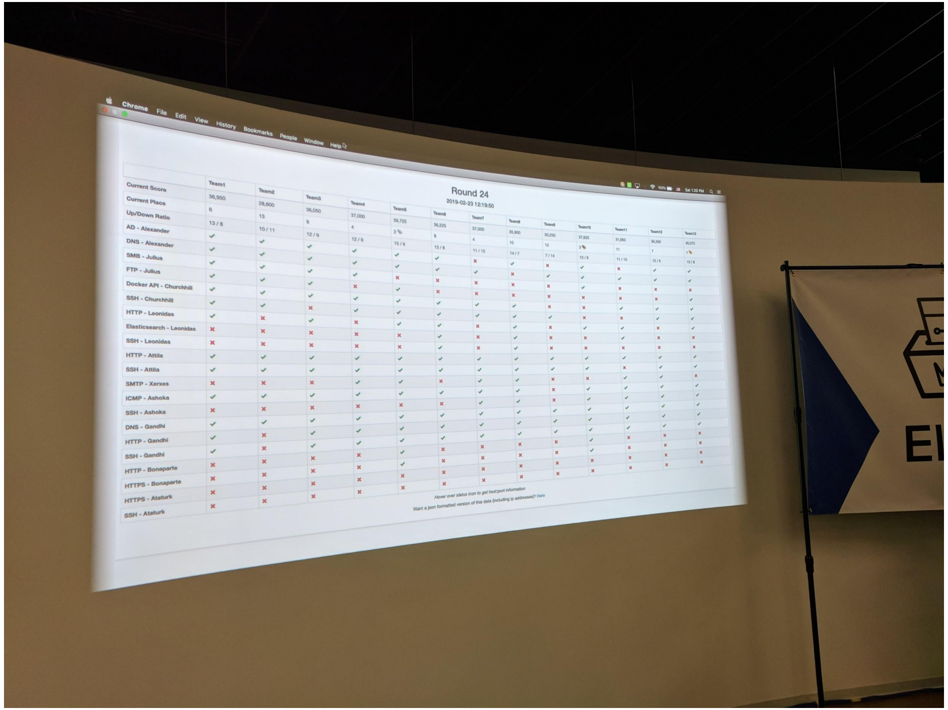
Cyber Defense Organization

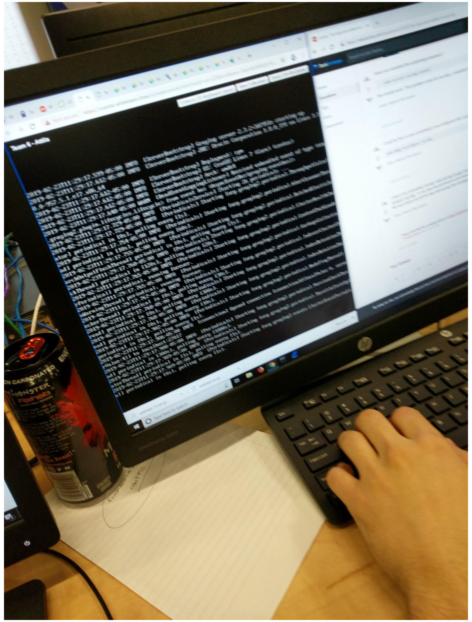
Fall 2018 - Firewalls

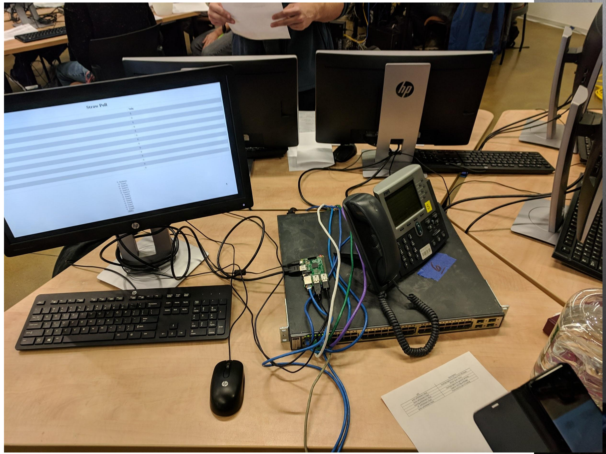
We went to a competition….
Information Security Talent Search 17 @Rochester Institute of Technology

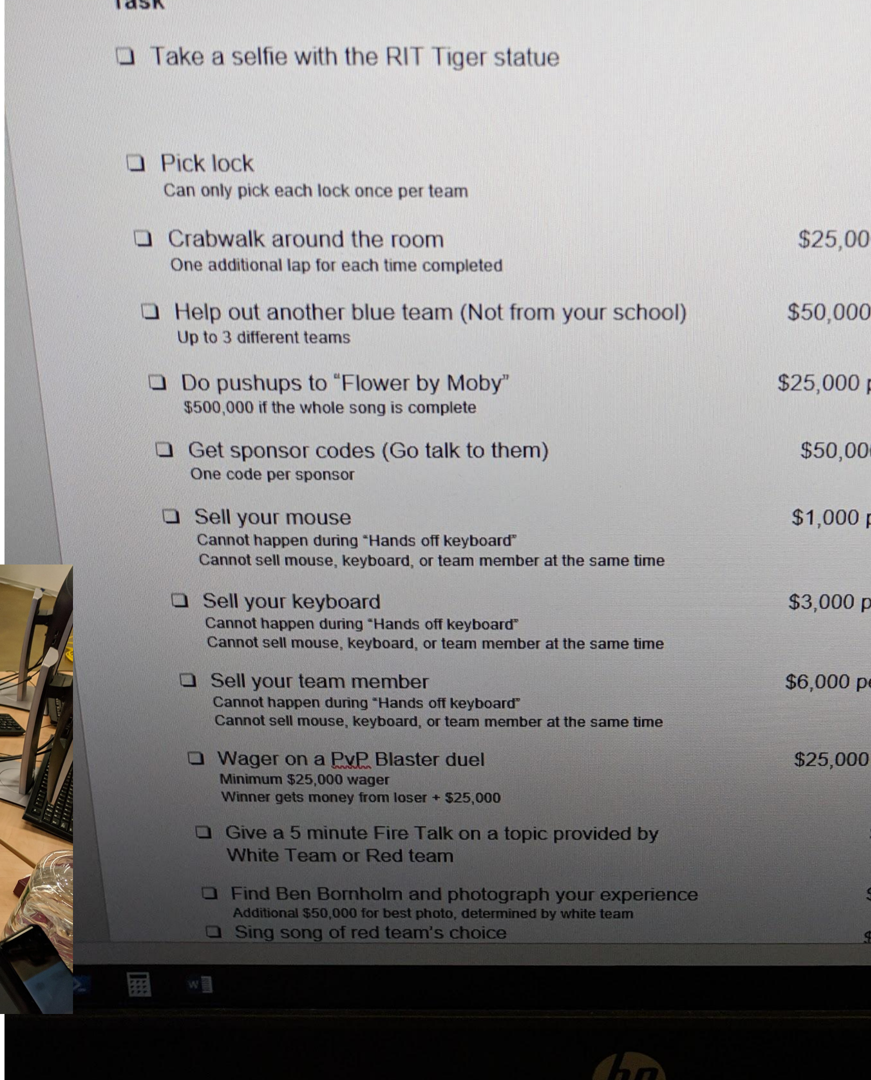


Some cool things that happened ...

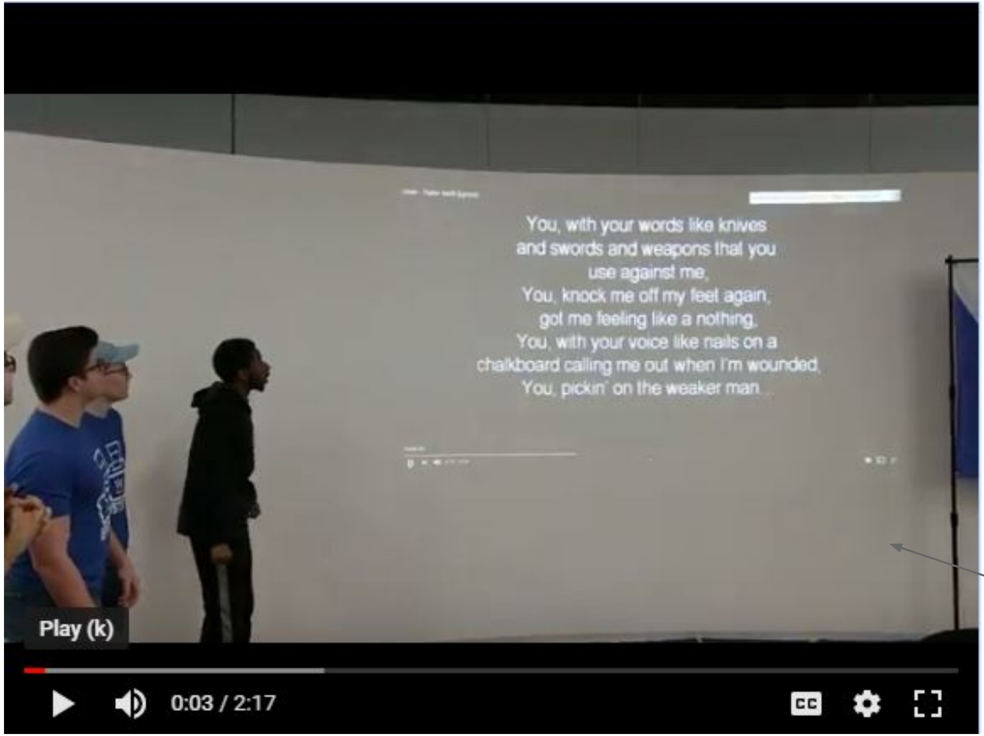
1) You can attack other team
2) You can call other teams
3) Lots of opportunities for points







And we have video of it…



Video of us singing Mean by Taylor Swift to get access to our servers back

Upcoming competitions

Central New York Hackathon sign up soon!(THIS WEEK)

- Beginner
- Sign up soon on http://www.cnyhackathon.org/
- DATES: Friday, April 5th, 4p to 9p
  Saturday, April 6th, 9a to 5p
-

Upcoming competitions

University at Buffalo Lockdown v7

Two teams
12 people total

What is Lockdown?

Lockdown is a cyber security competition hosted by UBNetDef, and set up in a defense only, Red vs Blue format. This semester's iteration of Lockdown is designed to be a beginner to intermediate skill level.

When is it?

Lockdown v6 is scheduled for **April 27, 2019 from 9AM to 5PM**. A schedule of events is located here.

Guest Speaker Sean Kelly

BlueCross BlueShield

Manager - Enterprise Information Risk Assurance at BlueCross BlueShield

MARCH 8th@2:00

Goals

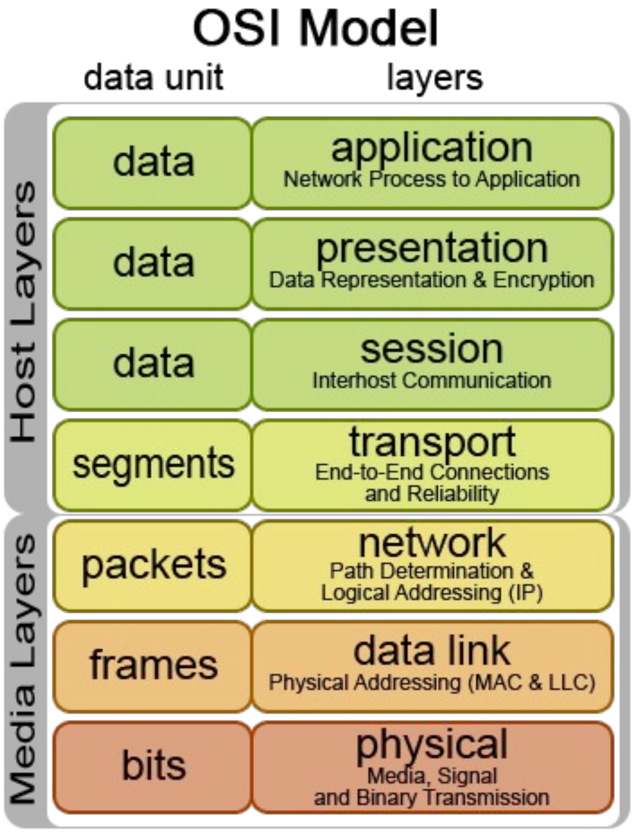
1. What are Firewalls
2. Basic Networking concepts
3. How firewalls blocks traffic
4. Setting up Firewall Rules
5. Firewall OS Examples
6. Cisco Packet Tracer Hands on

What are firewalls

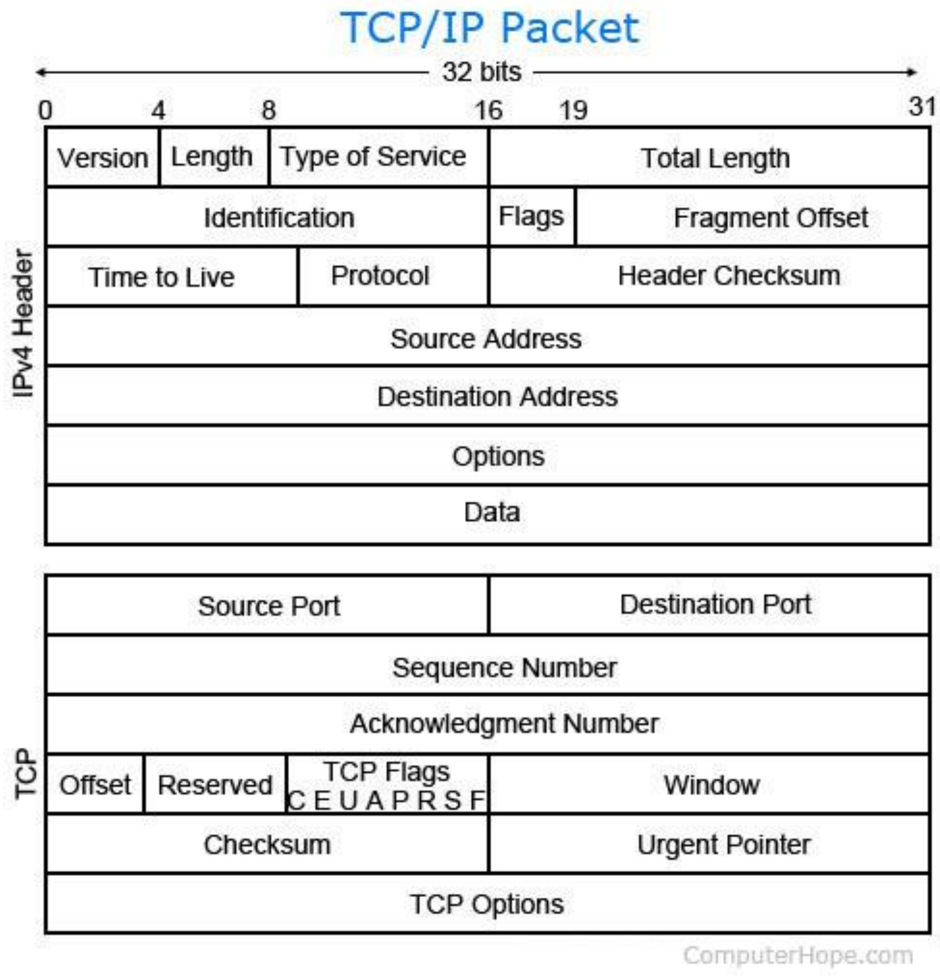
- The Overseer of the network
- Fancy definition
    - a part of a computer system or network which is designed to block unauthorized access while permitting outward communication.
- Most informed view of network traffic
- Most firewalls double as a router (and sometimes not)

Packets in Networking

- formatted unit of data carried by a packet-switched network
- Also called payload
- Packet switched network
- Encapsulation



Information



How Firewalls Block Traffic

- Different layers of the packet have different pieces of data
- The firewall has power of inspecting these layers
  - Information is power
  - Ports, Source IP address, and Destination IP Address,
- Firewall rules
  - Reflection of network needs and organizational needs
  - Element that abuses this information
  - Takes extreme advantage of network functions

Firewalls Available today

- Many available out there today:
  - PFSense
  - Palo Alto
  - Firewalld
  - Cisco ASA
  - And MORE

Let's Start the Fun Part!

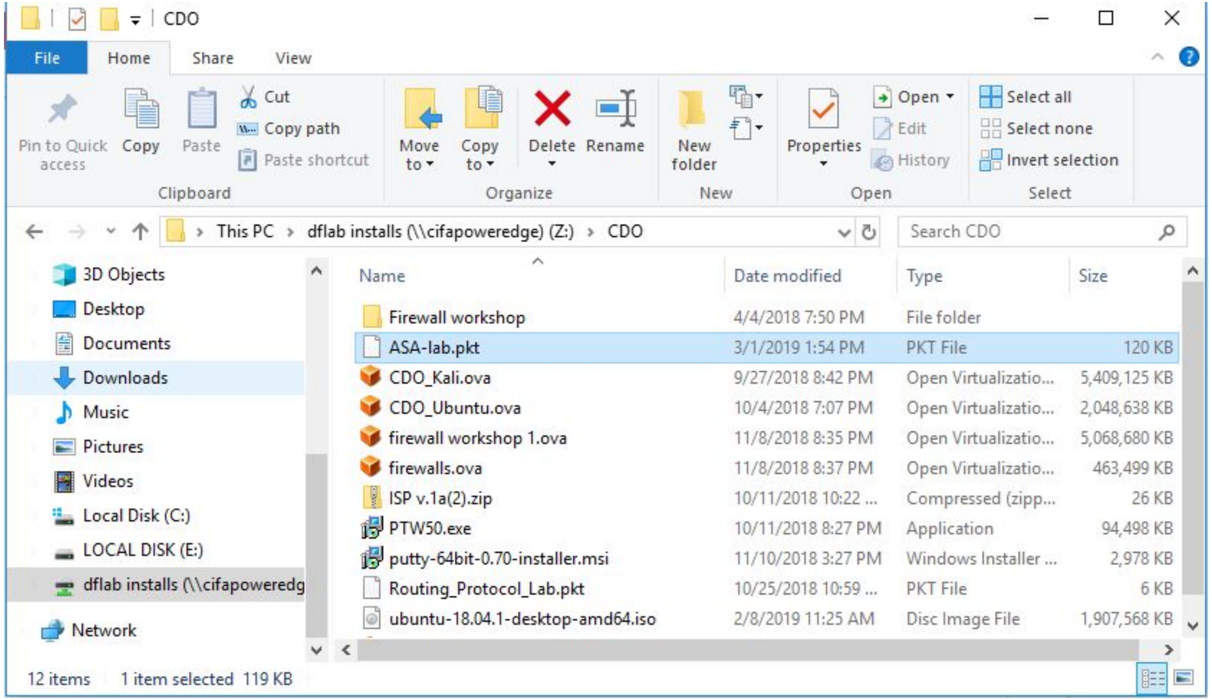
Cisco packet Tracer walkthrough!

Step 1: Open up Cisco Packet Tracer

- If you look on the desktop of the computer there should be an icon that looks like this: 

- Double Click!

Step 2: Download the ASA-lab.pkt file



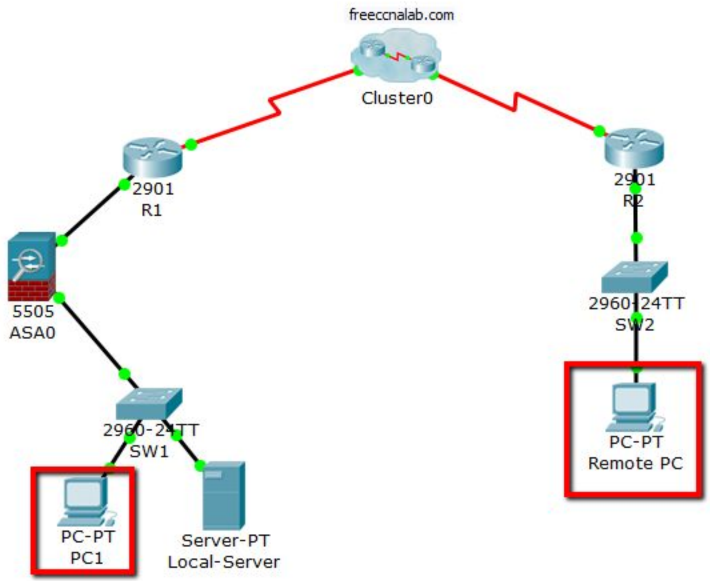
Step 3: We control Time!

- Once you downloaded and opened the file we will control time
- Please go to the bottom of the screen and click Fast-Forward time multiple times

- Once the interfaces turn green you are good

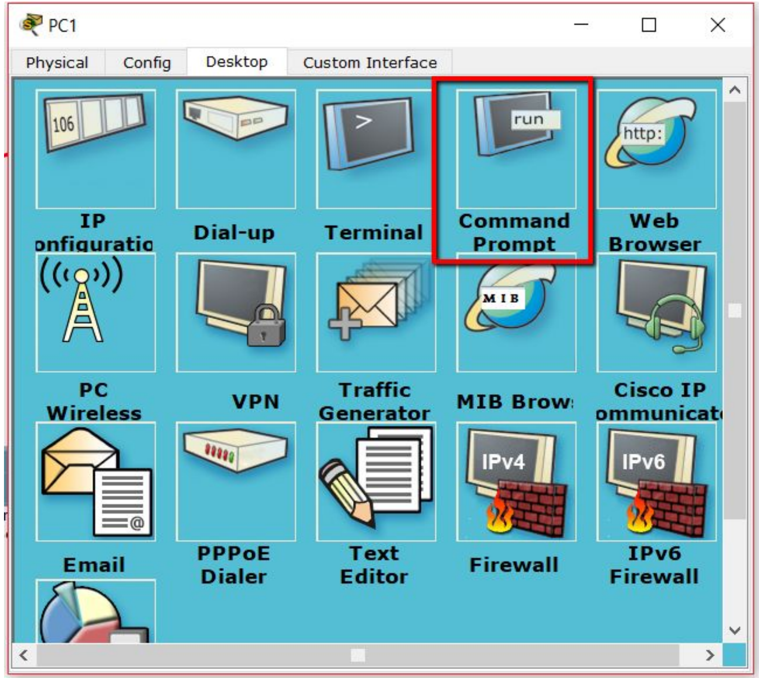
Step 4: Now we have access!

- We will be begin with PC1 and Remote pc!
- Double click to open them up



Step 5: See Traffic in the network

- In the desktop tab click Command Prompt
- Back on the cisco Packet tracer we need to switch to simulation mode
- Click:



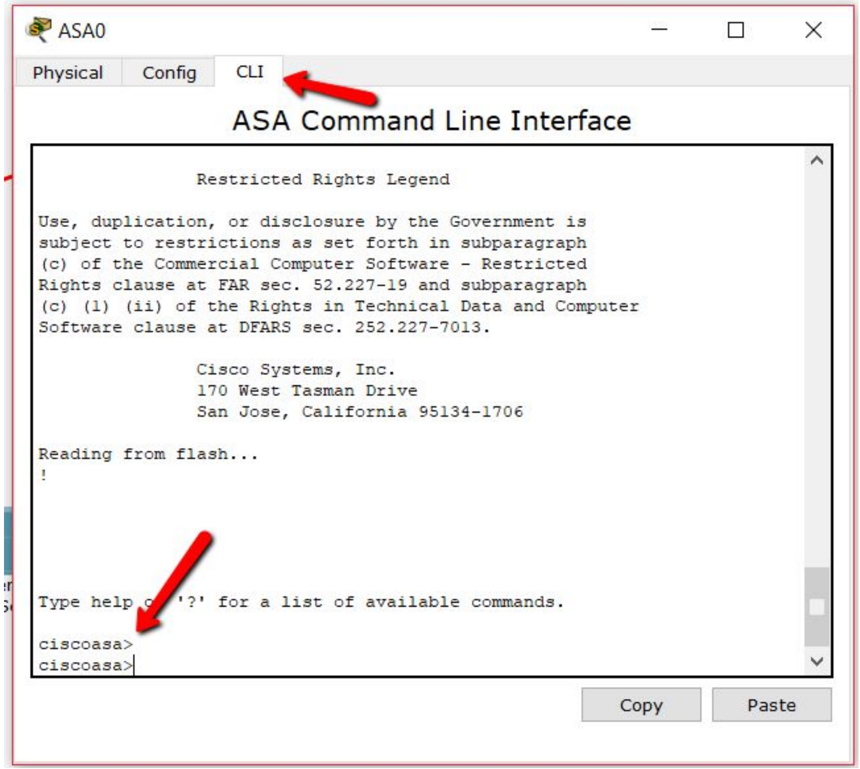
Step 6: Let's start pinging!

- PC1
  - ping 192.168.1.1 (Firewall)
  - ping 206.165.200.225 (Gateway)
- Remote PC
  - Ping 192.168.1.5 (Local PC)
- One at a time!
- Use Capture/Forward to watch the flow!

ComputerHope.com

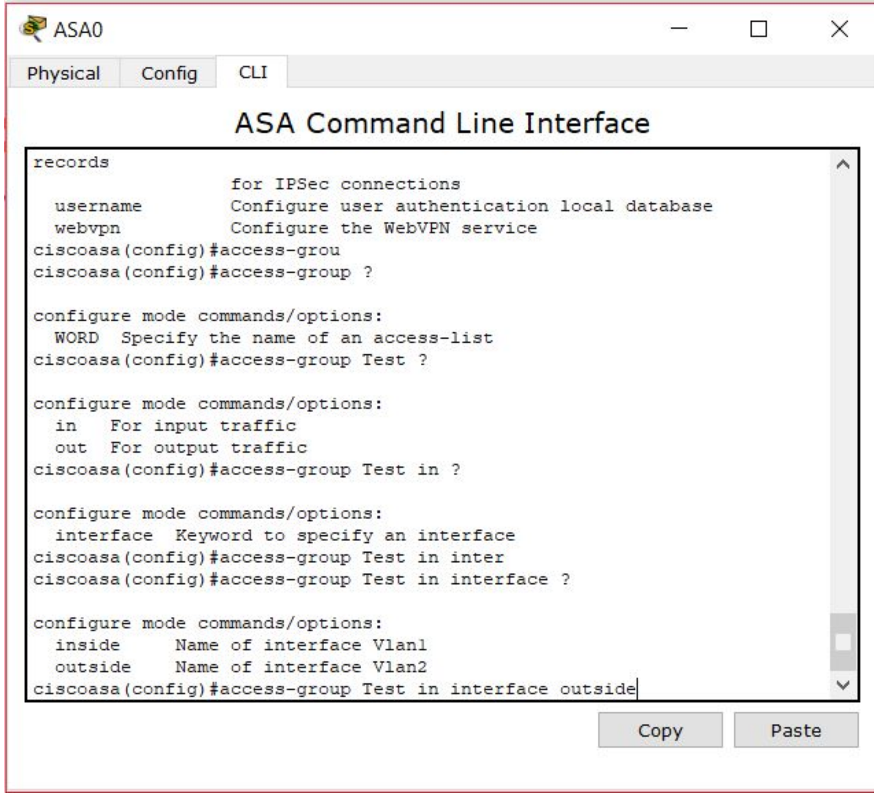
Step 7: It failed? Firewall Needs Fixing!

- Double click the ASA Box
- In the screen that opens choose CLI Tab
- **Type the below commands:**
  - **en <enter>**
  - **config t**
  - **access-list <Desired Name> extended permit icmp any any <Replace>**
    - **In replace do this 3 times for the following: echo, echo-reply, unreachable**



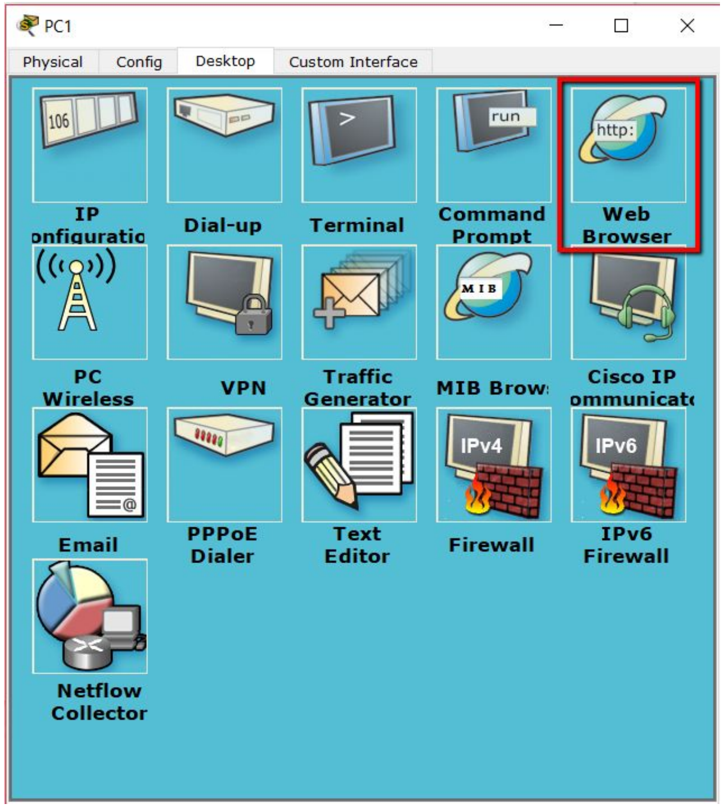
Step 8: Fixing Continued!

- After finishing the other commands finally type this one:
  - **access-group <Your ACL name> in interface outside**
- Last cmd: exit
- Try it pinging again now! :)
- DON’T CLOSE OUT YET



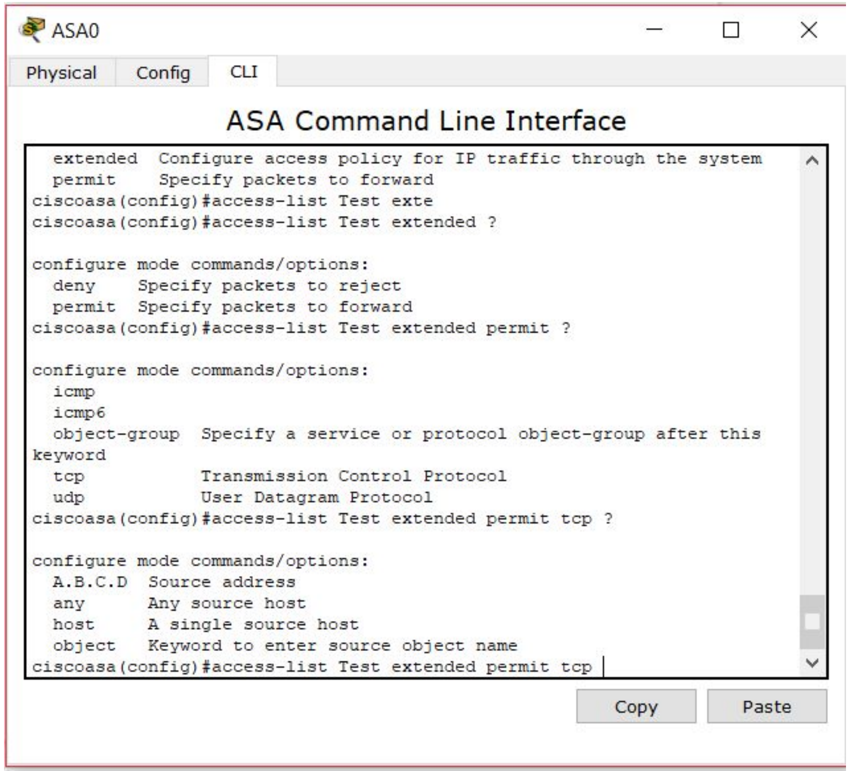
Step 9: There's more!

- Local PC should have access to a website named http://freeccnalab.com
- Let's head back to the desktop of the PC1 and this time choose Web Browser
- Try accessing the website in simulation mode!



Step 10: It failed again! More fixes!

- Sorry! I fail! Back to the ASA box CLI
- Follow these commands:
    - **en**
    - **config t**
    - **access-list <Previous name> extended permit tcp any any eq www**
    - **access-list <Previous name> extended permit tcp any any**



Step 11: Your all good!

- Your computer's should be able to do what is required!

Please Buy A T-Shirt

Guest Speaker!

Sean Kelly, Enterprise Information Risk Assurance Manager for BlueCross BlueShield of Western New York.

Sean has served multiple roles in the fields of Information Security, Risk and Controls Assurance, Audit and Consulting at various companies.

Please come!

Cya Next week!

Thank you to everyone who filled out the survey!

We made a discord! Keep an eye on email.

Follow us on Twitter? Add on myInvolvement?

MyInvolve

Twitter

Discord

CertStudy - Tuesday, 7:15pm
BB209

Sean Kelly - Friday - 2pm - BB151

March 5 - Jeffrey Baez - 7:30pm - Room TBA

https://discord.gg/9Dh6R5R