

Cyber Defense Organization

Fall 2018 - Firewalls



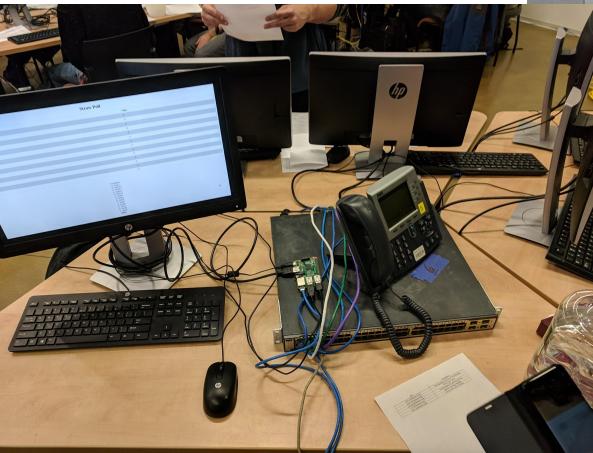
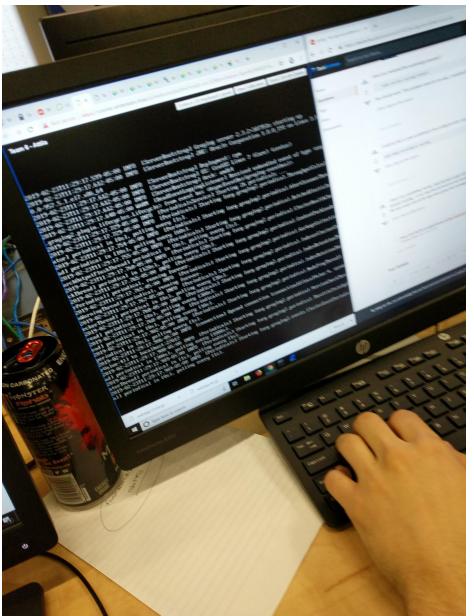
We went to a competition....

Information Security Talent Search 17 @Rochester Institute of Technology



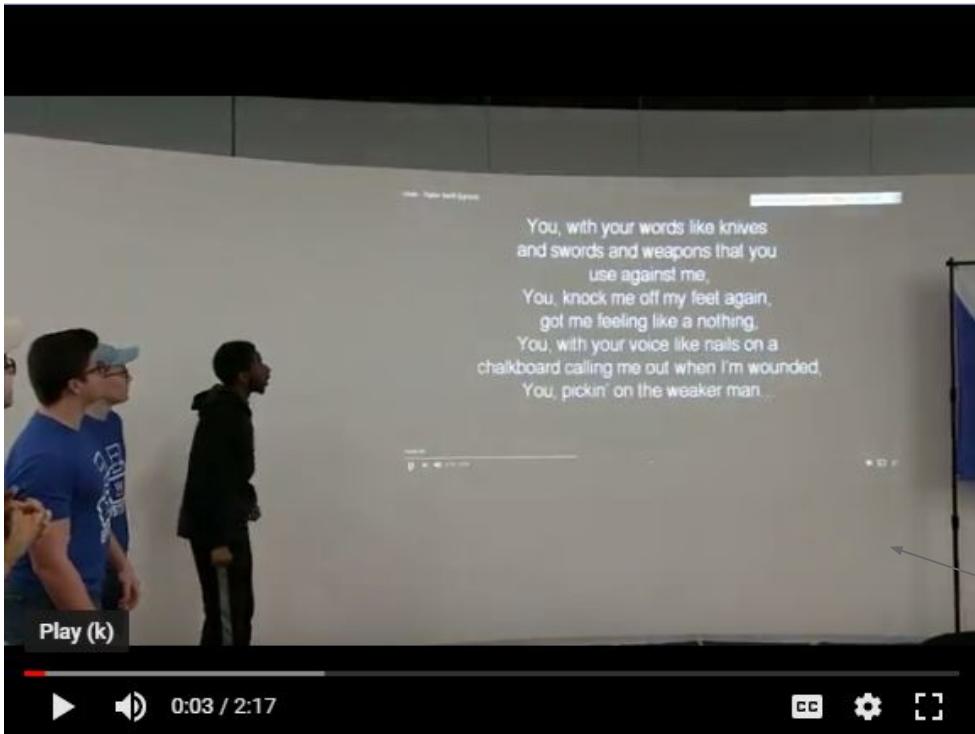
Some cool things that happened ...

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



Task	\$
<input type="checkbox"/> Take a selfie with the RIT Tiger statue	
<input type="checkbox"/> Pick lock Can only pick each lock once per team	
<input type="checkbox"/> Crabwalk around the room One additional lap for each time completed	\$25,000
<input type="checkbox"/> Help out another blue team (Not from your school) Up to 3 different teams	\$50,000
<input type="checkbox"/> Do pushups to "Flower by Moby" \$500,000 if the whole song is complete	\$25,000 p
<input type="checkbox"/> Get sponsor codes (Go talk to them) One code per sponsor	\$50,000
<input type="checkbox"/> Sell your mouse Cannot happen during "Hands off keyboard" Cannot sell mouse, keyboard, or team member at the same time	\$1,000 p
<input type="checkbox"/> Sell your keyboard Cannot happen during "Hands off keyboard" Cannot sell mouse, keyboard, or team member at the same time	\$3,000 p
<input type="checkbox"/> Sell your team member Cannot happen during "Hands off keyboard" Cannot sell mouse, keyboard, or team member at the same time	\$6,000 p
<input type="checkbox"/> Wager on a PvP Blaster duel Minimum \$25,000 wager Winner gets money from loser + \$25,000	\$25,000
<input type="checkbox"/> Give a 5 minute Fire Talk on a topic provided by White Team or Red team	
<input type="checkbox"/> Find Ben Bornholm and photograph your experience Additional \$50,000 for best photo, determined by white team	
<input type="checkbox"/> Sing song of red team's choice	

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

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](#).

Two teams
12 people total



Guest Speaker Sean Kelly

CYBER DEFENSE ORGANIZATION

COME SPEAK WITH
SEAN KELLY

MANAGER OF
ENTERPRISE
INFORMATION
RISK ASSURANCE

MARCH 8TH 2:00
ROOM BB151



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



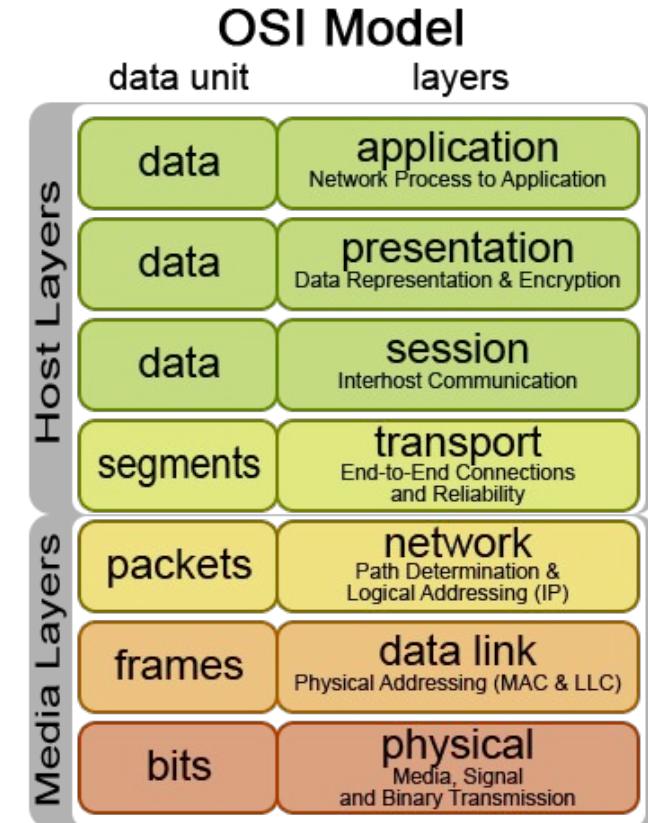
What are firewalls

- 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)



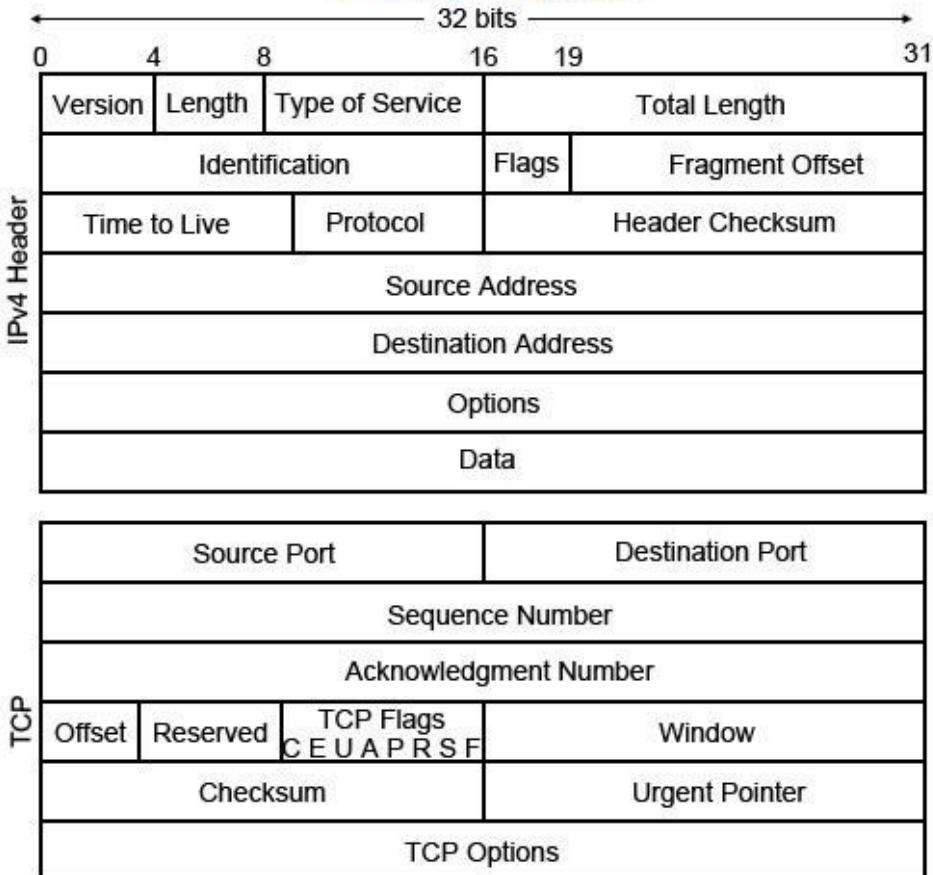
Packets in Networking

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



Information

TCP/IP Packet



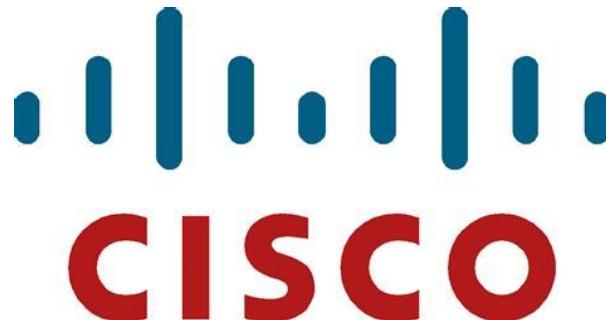
How Firewalls Block Traffic

- 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!**

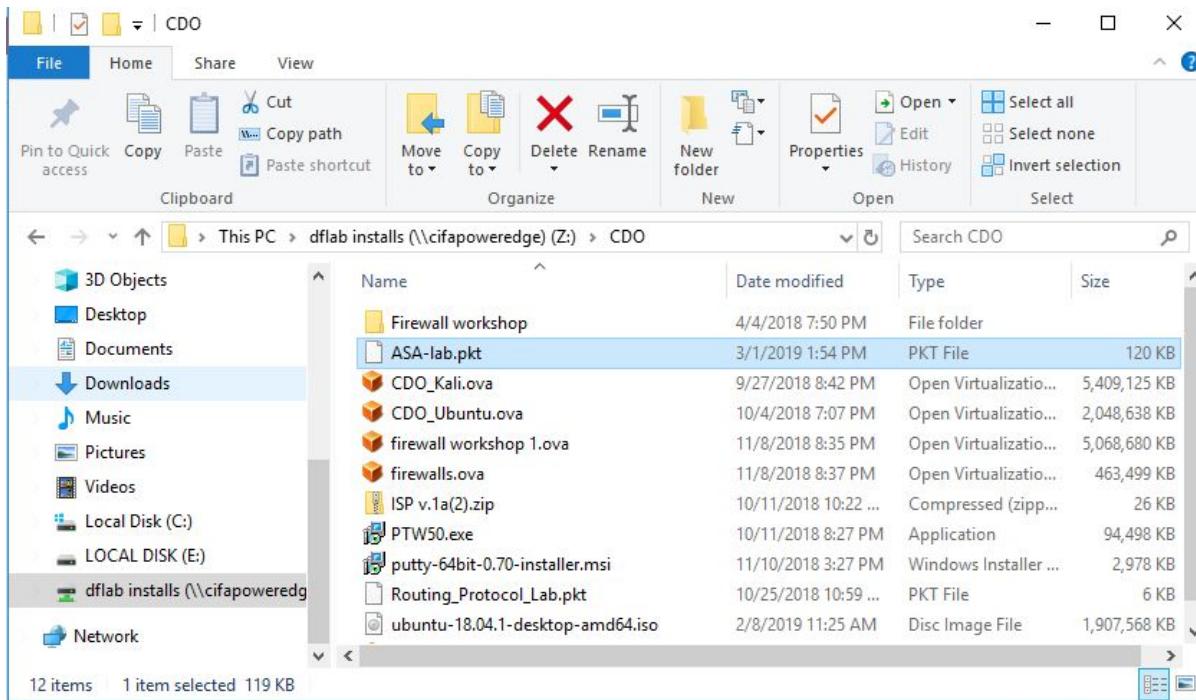
Step 1: Open up Cisco Packet Tracer

- 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!

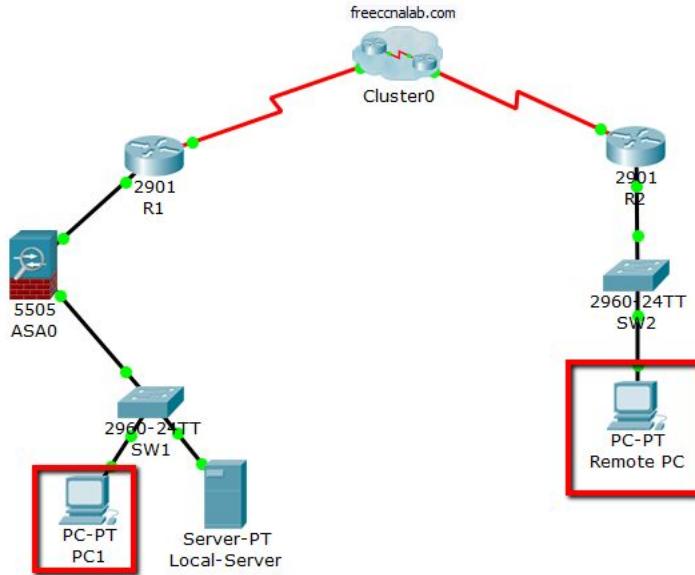
- Once you downloaded and opened the file we will control time
- Please go to the bottom of the screen and click Fast-Forward time multiple times



- Once the interfaces turn green you are good

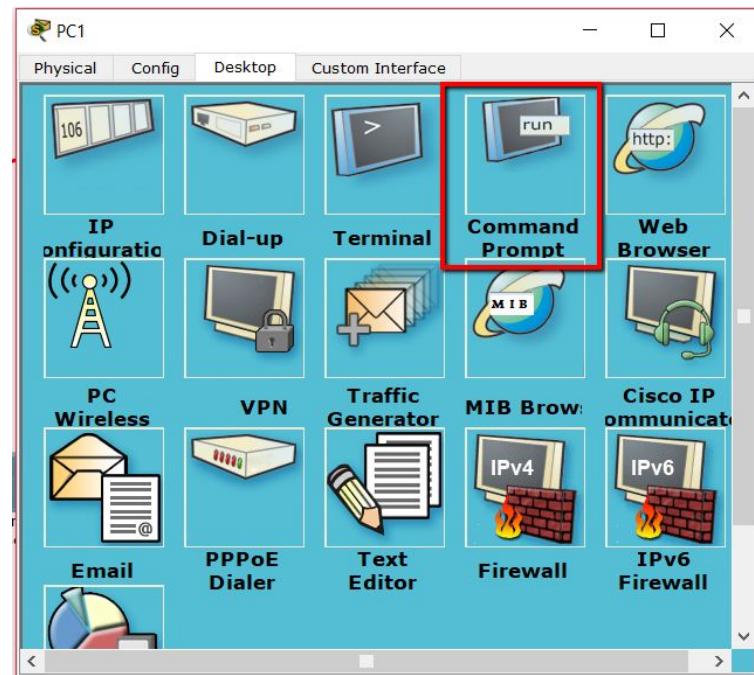
Step 4: Now we have access!

- We will 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:



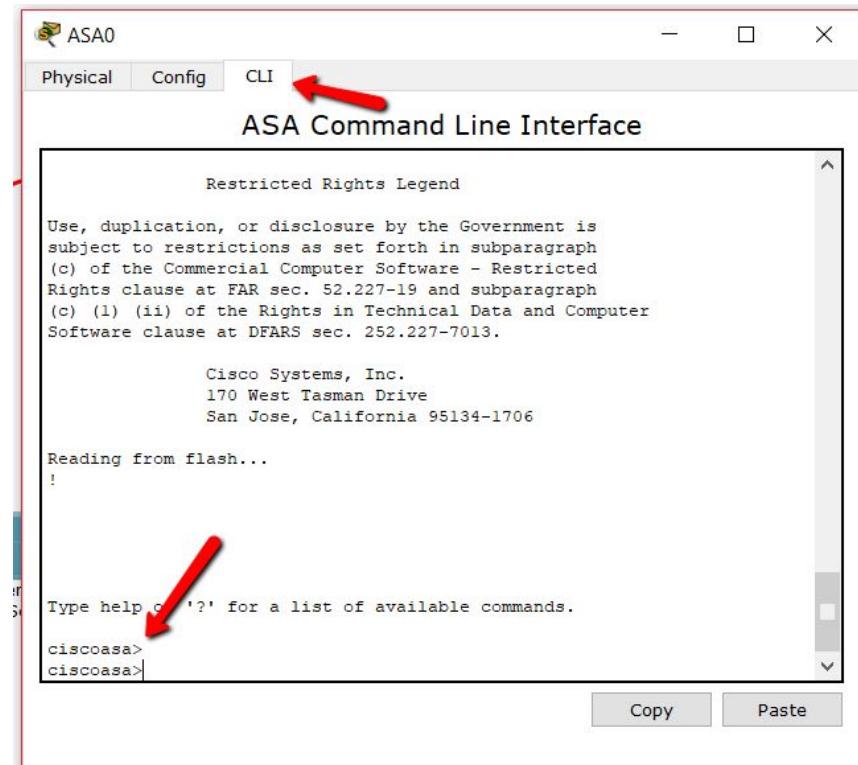
Step 6: Let's start pinging!

- 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!



Step 7: It failed? Firewall Needs Fixing!

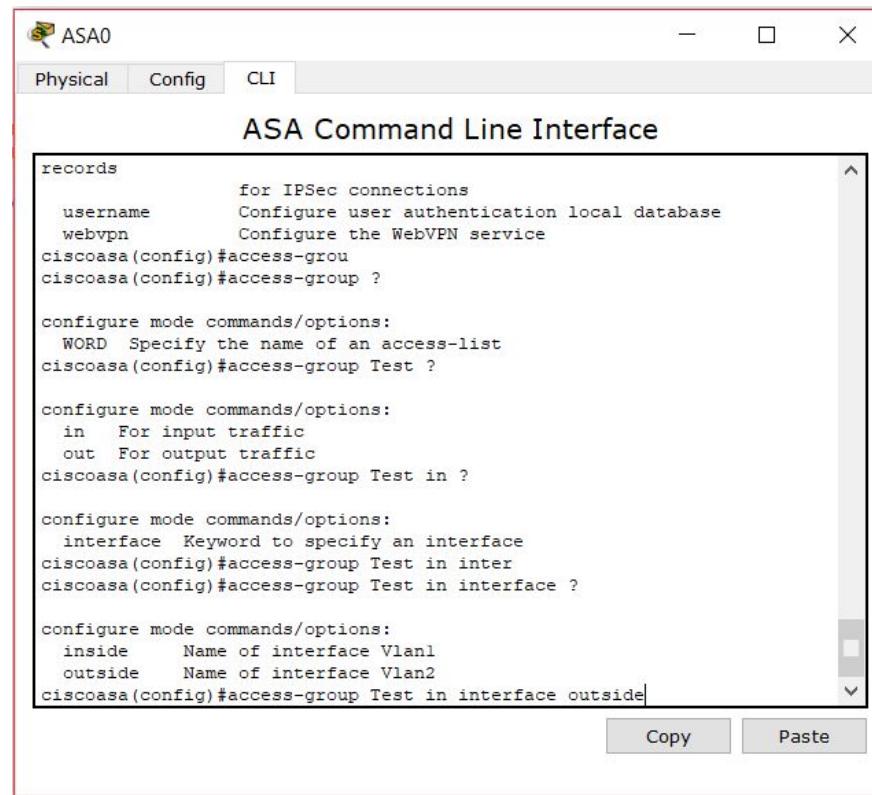
- Double click the ASA Box
- In the screen that opens choose CLI Tab
- **Type the below commands:**
 - **en <enter>**
 - **config t**
 - **access-list <Desired Name> extended**
permit icmp any any <Replace>
 - In replace do this 3 times for the following: echo, echo-reply, unreachable



The screenshot shows the ASA Command Line Interface window. The title bar says "ASA0" and "ASA Command Line Interface". The "CLI" tab is highlighted with a red arrow. The main area displays the ASA Command Line interface. It includes a "Restricted Rights Legend" and copyright information for Cisco Systems, Inc. Below that, it says "Reading from flash...". At the bottom, it shows the command line prompt "ciscoasa>" followed by a help message: "Type help or '?' for a list of available commands." There are "Copy" and "Paste" buttons at the bottom right.

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



The image shows a screenshot of the ASA Command Line Interface (CLI) window titled "ASA0". The window has tabs for "Physical", "Config", and "CLI", with "CLI" selected. The main area displays a command history or log:

```
records
for IPSec connections
username      Configure user authentication local database
webvpn       Configure the WebVPN service
ciscoasa(config)#access-grou
ciscoasa(config)#access-group ?

configure mode commands/options:
WORD Specify the name of an access-list
ciscoasa(config)#access-group Test ?

configure mode commands/options:
in   For input traffic
out  For output traffic
ciscoasa(config)#access-group Test in ?

configure mode commands/options:
interface Keyword to specify an interface
ciscoasa(config)#access-group Test in inter
ciscoasa(config)#access-group Test in interface ?

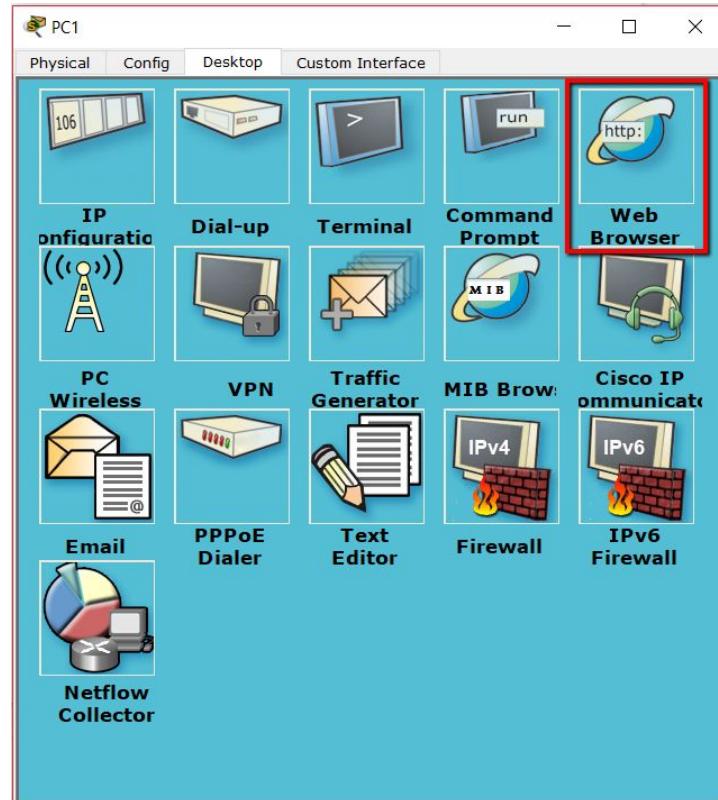
configure mode commands/options:
inside    Name of interface Vlan1
outside   Name of interface Vlan2
ciscoasa(config)#access-group Test in interface outside

ciscoasa(config)#access-group Test in interface outside
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons.

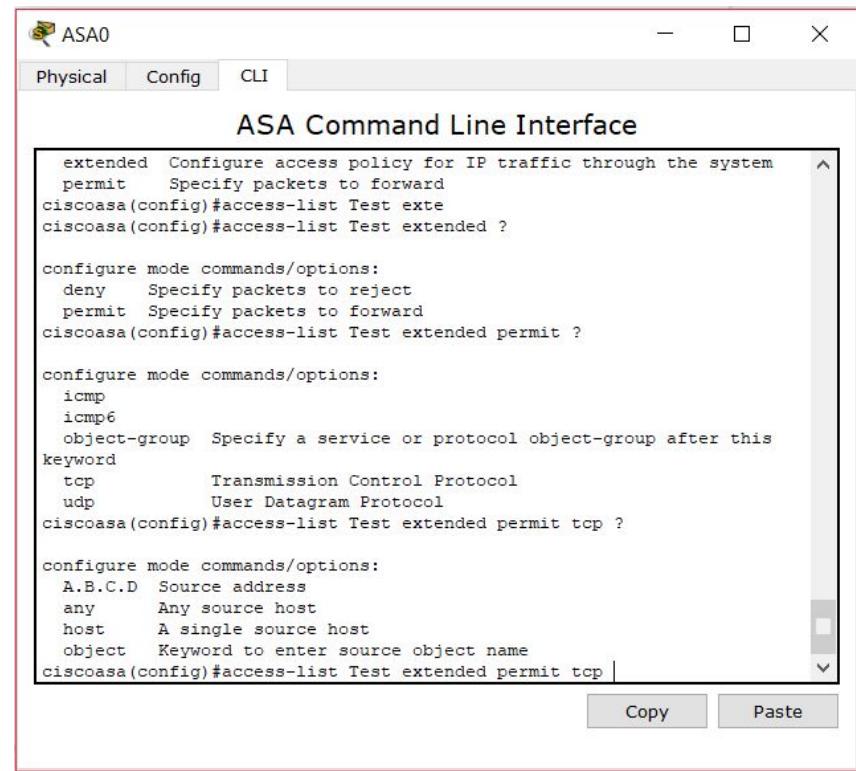
Step 9: There's more!

- Local PC should have access to a website named <http://freecnclab.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



The image shows a screenshot of the ASA Command Line Interface (CLI) window titled "ASA0". The window has tabs for "Physical", "Config", and "CLI", with "CLI" selected. The main area displays a command history or help output for the "access-list" command. The text is as follows:

```
extended  Configure access policy for IP traffic through the system
permit   Specify packets to forward
ciscoasa(config)#access-list Test exte
ciscoasa(config)#access-list Test extended ?

configure mode commands/options:
deny    Specify packets to reject
permit   Specify packets to forward
ciscoasa(config)#access-list Test extended permit ?

configure mode commands/options:
icmp
icmp6
object-group  Specify a service or protocol object-group after this
keyword
tcp       Transmission Control Protocol
udp       User Datagram Protocol
ciscoasa(config)#access-list Test extended permit tcp ?

configure mode commands/options:
A.B.C.D  Source address
any      Any source host
host     A single source host
object   Keyword to enter source object name
ciscoasa(config)#access-list Test extended permit tcp |
```

At the bottom of the window are "Copy" and "Paste" buttons.

Step 11: You're all good!

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



Please Buy A T-Shirt



CYBER DEFENSE ORGANIZATION

**COME SPEAK WITH
SEAN KELLY**

**MANAGER OF
ENTERPRISE
INFORMATION
RISK ASSURANCE**

**MARCH 8TH 2:00
ROOM BB151**



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?



 MyInvolvement



 Twitter



 Discord



CertStudy - Tuesday, 7:15pm
BB209

**Sean Kelly - Friday - 2pm -
BB151**

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

<https://discord.gg/9Dh6R5R>