“This simulation shows how basic firewall-like rules

can be used to control network traffic at the router level.

Access Control Lists (ACLs) and Port Security were configured

to mimic common real-world cybersecurity defenses.”

How to Test This Project (Ping + Block + Unblock)

1. Open the .pkt file in Cisco Packet Tracer.

**To test normal ping (before blocking):**

* Click on PC0 (the attacker)
* Go to the Desktop tab and open Command Prompt
* Type: ping 192.168.2.10
* You should see replies like: "Reply from 192.168.2.10..."

**To block the attacker using ACL:**

* Click on Router1 (the router connected to the defender side)
* Go to the CLI tab
* Type the following commands one by one:

enable  
 configure terminal  
 access-list 100 deny icmp 192.168.1.0 0.0.0.255 any  
 access-list 100 permit ip any any  
 interface fastEthernet0/0  
 ip access-group 100 in  
 exit

* Go back to PC0 and ping 192.168.2.10 again
* You should now see: "Request timed out" or "Destination host unreachable"

**To allow the ping again (remove the block):**

* Go back to Router1
* In the CLI tab, type:

enable  
 configure terminal  
 interface fastEthernet0/0  
 no ip access-group 100 in  
 exit

* Go back to PC0 and ping 192.168.2.10 again
* You should now get replies again