

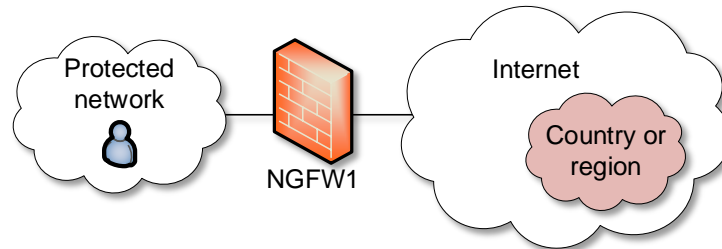
# Geolocation and Geoblocking

Nathan Long, Ty Love-Baker  
Advisor: Jorge Crichigno, Ali ALSabeh

## 1. Introduction

*Geolocation* is the estimation of the real-world geographic location of an object. Modern Next-generation Firewalls (NGFWs) have the capability of tracking the physical location of a device attempting to connect to the network they are protecting. *Geoblocking* is when NGFWs *restrict* or *allow* access to content based on the geolocation.

This project will explore the use of geoblocking and its effectiveness. The project must build a security policy using diverse geolocations (countries and regions. E.g., China, Russia, Brazil, South America, the entire world but U.S.) and test those rules.



**Figure 1.** Example of geolocation. The firewall NGFW1 protects the internal network from countries or regions specified by the security engineer.

## 2. Research Challenge

The research challenge is to protect the internal network, using a NGFW and geoblocking. Figure 1 shows an example of a NGFW using geoblocking to prevent users from a country or region. Note that an additional challenge is to block attackers from using online proxies and/or anonymizers. These are tools that are freely available online, and as their names indicate, they anonymize their traffic.