# 用 iptables 拒絕特定國家連線

# 用 iptables 拒絕特定國家連線

1. **電算中心莊宜諺**
2. **2018年5月7日**

# 原來可以用 iptables 拒絕特定國家連線!!!

## 請愛用 xtables-addons

# 什麼情況下需要使用

* 使用者只來自於特定國家
* 阻擋來自特定國家的 DDOS 攻擊
* 不允許傳輸至特定國家
  + 機密
  + 授權
* 好處
  + 安全
  + LOG少

# 需求

* gcc gcc-c++ make automake
* zip xz wget unzip
* iptables-devel perl-Text-CSV\_XS
* kernel–devel
  + 注意: kernel-devel 與 kernel 及其它安裝的 kernel- 版本需要一致
  + 若安裝了新版的的 kernel , 重開機才會生效

# 怎麼安裝

## YUM 能裝嗎? 沒有 RPM 嗎?

* ~~RPMFUSION 有提供 YUM REPO 及 RPM , 但只有特定一個 kernel 版能裝~~

## Debian/Ubuntu呢?

* 簡單很多, 直接由 apt-get 安裝

# 從 Source Code 安裝

* OS: CentOS 7
* 在 ./configure & make & make install 之前, 需要移除 TARPIT module
  + 因為編編不成功, 同時也不常用到
* cheat script

cd /usr/local/src

curl -O https://in.ncu.edu.tw/center31/xtables-addons.sh

chmod a+x ./xtables-addons.sh

./xtables-addons.sh

# 每月自動更新國家<->IP資料庫

* GEOIP

cd /usr/local/src/xtables-addons-2.14/geoip

./xt\_geoip\_dl

./xt\_geoip\_build -D /usr/share/xt\_geoip \*.csv



